Mandiant

VBR20260121 - JANUARY 21, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VBR20260121. This content pack requires Director version 4.14.1.0-0 or higher.

If you've enabled the Content Service, this content pack will automatically download and be applied to your Director (see **The Mandiant Content Service** (https://docs.mandiant.com/home/msv-mandiant-content-service) and **Managing Security Validation Content** (https://docs.mandiant.com/home/msv-content-settings) for full details). Otherwise, you can download the **security content pack** (https://docs.mandiant.com/home/msv-content-packs) from the Mandiant Documentation Portal.

Summary of Changes

- 634 Actions retired
- 5 Sequences retired
- 8 Evaluations retired
- 3662 Actions updated
- 48 Sequences updated
- 17 Evaluations updated
- 959 Files updated

Release Highlights

- Updated all content metadata to conform to current standards.

Retired Security Content

With this release, 634 Actions, 5 Sequences, and 8 Evaluations have been retired.

Actions

VID	Name	Reason for Removal
A100-364	Benign DNS Query - Google.com	Content no longer meets Validation's standards of use
A102-337	Command and Control - BEACON, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-341	Command and Control - CEELOADER, DNS Query #2	Content no longer meets Validation's standards of use
A102-344	Command and Control - BEACON, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-359	Command and Control - CEELOADER, DNS Query #1	Content no longer meets Validation's standards of use
A102-364	Command and Control - FIN13, SWEARJAR, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-416	Command and Control - KEYSHOW, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-474	Command and Control - SPRINGBEE, DNS Query, Variant #3	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A102-477	Command and Control - SPRINGBEE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-479	Command and Control - SPRINGBEE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-483	Command and Control - FUSIONDRIVE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-494	Command and Control - LOUDSTEP, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-509	Command and Control - CARBANAK, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-510	Command and Control - METASTAGE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-511	Command and Control - DRIFTPIN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-527	Command and Control - LINKSPAN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-538	Command and Control - LOUDSTEP, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-539	Command and Control - LOUDSTEP, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-540	Command and Control - LOUDSTEP, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-544	Command and Control - GH0ST, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-559	Command and Control - TERMITE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-562	Command and Control - GRAMDOOR, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-601	Command and Control - SMOKELOADER, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A102-602	Command and Control - SMOKELOADER, DNS Query, Variant #7	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A102-603	Command and Control - SMOKELOADER, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A102-604	Command and Control - SMOKELOADER, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A102-605	Command and Control - SMOKELOADER, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-606	Command and Control - SMOKELOADER, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-607	Command and Control - SMOKELOADER, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-608	Command and Control - SMOKELOADER, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-653	Command and Control - TEMP.Armageddon, QUIETSIEVE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-654	Command and Control - TEMP.Armageddon, DESSERTDOWN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-655	Command and Control - TEMP.Armageddon, PTERODO, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-656	Command and Control - TEMP.Armageddon, DINOTRAIN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-659	Command and Control - TEMP.Armageddon, OBFUBERRY, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-665	Command and Control - AGENTTESLA, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-666	Command and Control - EMOTET, DNS Query, Variant #17	Content no longer meets Validation's standards of use
A102-670	Command and Control - LOKIBOT, DNS Query, Variant #3	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A102-671	Command and Control - LOKIBOT, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-672	Command and Control - LOKIBOT, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A102-673	Command and Control - LOKIBOT, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A102-674	Command and Control - LOKIBOT, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A102-675	Command and Control - MOUSEISLAND, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A102-677	Command and Control - NANOCORE, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-695	Command and Control - EMOTET, DNS Query, Variant #16	Content no longer meets Validation's standards of use
A102-698	Command and Control - APT1, AUSOV, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-699	Command and Control - APT1, BANGAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-700	Command and Control - APT1, BANGAT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-701	Command and Control - APT1, BIGWHEEL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-702	Command and Control - APT1, BIGWHEEL, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-703	Command and Control - APT1, BIGWHEEL, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-704	Command and Control - APT1, BIGWHEEL, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-705	Command and Control - APT1, BISCUIT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-706	Command and Control - APT1, BISCUIT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-707	Command and Control - APT1, BISCUIT, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-708	Command and Control - APT1, BISCUIT, DNS Query, Variant #4	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A102-709	Command and Control - APT1, COOKIEBAG, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-710	Command and Control - APT1, CSPLUGIN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-711	Command and Control - APT1, GOGGLES, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-712	Command and Control - APT1, GOGGLES, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-713	Command and Control - APT1, GREENCAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-714	Command and Control - APT1, GREENCAT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-715	Command and Control - APT1, GREENCAT, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-716	Command and Control - APT1, GREENCAT, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-717	Command and Control - APT1, HACKSFASE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-718	Command and Control - APT1, HACKSFASE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-719	Command and Control - APT1, HACKSFASE, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-720	Command and Control - APT1, HACKSFASE, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-721	Command and Control - APT1, HELAUTO, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-722	Command and Control - APT1, HELAUTO, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-723	Command and Control - APT1, KIDSTABLE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-724	Command and Control - APT1, KIDSTABLE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-725	Command and Control - APT1, LONGTHROW, DNS Query, Variant #1	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A102-726	Command and Control - APT1, LONGTHROW, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-727	Command and Control - APT1, LONGTHROW, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-728	Command and Control - APT1, MINIASP, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-729	Command and Control - APT1, RAVETIME, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-730	Command and Control - APT1, SOGU, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-731	Command and Control - APT1, TARSIP, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-732	Command and Control - APT1, TARSIP, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-733	Command and Control - APT1, TARSIP, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-734	Command and Control - APT1, TARSIP, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-735	Command and Control - APT1, WARP, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-736	Command and Control - APT1, ZERODUE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-737	Command and Control - APT1, ZERODUE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-738	Command and Control - APT16, ELMER, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-739	Command and Control - APT16, PAINTPLUG, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-740	Command and Control - APT16, PAINTPLUG, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-741	Command and Control - APT16, PROTUX, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-742	Command and Control - APT16, PROTUX, DNS Query, Variant #2	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A102-743	Command and Control - APT16, PROTUX, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-744	Command and Control - APT16, TABCTENG, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-745	Command and Control - APT16, TABCTENG, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-746	Command and Control - APT16, TABCTENG, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-747	Command and Control - APT16, TABCTENG.BIN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-748	Command and Control - APT16, TABCTENG.BIN, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-749	Command and Control - APT16, UNICAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-750	Command and Control - UNC2190, BEACON, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-751	Command and Control - UNC2190, BEACON, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-752	Command and Control - UNC2190, BEACON, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-753	Command and Control - UNC2190, BEACON, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-754	Command and Control - UNC2190, BEACON, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A102-755	Command and Control - UNC2190, BEACON, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A102-756	Command and Control - UNC2190, BEACON, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A102-757	Command and Control - UNC2190, BEACON, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A102-758	Command and Control - UNC2190, BEACON, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A102-759	Command and Control - UNC2190, DNS Query, Variant #2	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A102-825	Command and Control - APT18, COBALT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-826	Command and Control - APT18, COBALT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-827	Command and Control - APT18, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-829	Command and Control - APT18, POISONIVY, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-830	Command and Control - APT18, QUICKBALL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-831	Command and Control - APT18, TWOSEAM, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-835	Command and Control - APT30, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-836	Command and Control - APT30, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-839	Command and Control - TEMP.Vermin, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-840	Command and Control - TEMP.Vermin, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-841	Command and Control - TEMP.Vermin, RATVERMIN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-842	Command and Control - TEMP.Vermin, RATVERMIN, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-843	Command and Control - TEMP.Vermin, RATVERMIN, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-844	Command and Control - TEMP.Vermin, RATVERMIN, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-845	Command and Control - TEMP.Vermin, SPECTRUM, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-846	Command and Control - TEMP.Vermin, SPECTRUM, DNS Query, Variant #2	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A102-847	Command and Control - TEMP.Vermin, SPECTRUM, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-848	Command and Control - TEMP.Vermin, SPECTRUM, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A102-945	Command and Control - BABUK, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-946	Command and Control - BABUK, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-948	Command and Control - APT28, XTUNNEL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-949	Command and Control - APT28, SOURFACE.CORESHELL, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-950	Command and Control - APT28, SOURFACE.CORESHELL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-951	Command and Control - APT28, NIGHTCALL, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-952	Command and Control - APT28, NIGHTCALL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-953	Command and Control - APT28, KOADIC, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-954	Command and Control - APT28, GAMEFISH, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-955	Command and Control - APT28, GAMEFISH, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-956	Command and Control - APT28, GAMEFISH, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-957	Command and Control - APT28, EVILTOSS, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-958	Command and Control - APT28, EVILTOSS, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-959	Command and Control - APT28, EVILTOSS, DNS Query, Variant #1	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A102-963	Command and Control - WHITEBEAR, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-964	Command and Control - WHITEBEAR, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-965	Command and Control - WHITEBEAR, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-974	Command and Control - Turla Team, SUPERGLUE, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-975	Command and Control - Turla Team, SUPERGLUE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-976	Command and Control - Turla Team, SUPERGLUE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-977	Command and Control - Turla Team, BIRDPEN.AIRMAIL, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-978	Command and Control - Turla Team, BIRDPEN.AIRMAIL, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-979	Command and Control - Turla Team, BIRDPEN.AIRMAIL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-980	Command and Control - Turla Team, BIRDPEN, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A102-981	Command and Control - Turla Team, BIRDPEN, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A102-982	Command and Control - Turla Team, BIRDPEN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A102-996	Command and Control - APT45, QUINSTATUS, Malicious DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-009	Command and Control - TEMP.Hex, POISONIVY, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-010	Command and Control - TEMP.Hex, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-011	Command and Control - TEMP.Hex, DNS Query, Variant #2	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-012	Command and Control - TEMP.Hex, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-013	Command and Control - TEMP.Hex, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-014	Command and Control - TEMP.Hex, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-015	Command and Control - TEMP.Hex, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-016	Command and Control - TEMP.Hex, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A103-017	Command and Control - TEMP.Hex, HOMEUNIX, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-018	Command and Control - TEMP.Hex, SOGU, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-019	Command and Control - TEMP.Hex, SOGU, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-038	Command and Control - BIRDWATCH, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-039	Command and Control - BIRDWATCH, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-040	Command and Control - BIRDWATCH, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-041	Command and Control - BIRDWATCH, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-042	Command and Control - BIRDWATCH, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-044	Command and Control - FIN7, LOADOUT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-045	Command and Control - FIN7, LOADOUT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-046	Command and Control - FIN7, LOADOUT, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-047	Command and Control - FIN7, LOADOUT, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-048	Command and Control - FIN7, LOADOUT, DNS Query, Variant #5	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-050	Command and Control - FIN7, POWERPLANT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-051	Command and Control - FIN7, POWERPLANT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-052	Command and Control - FIN7, POWERPLANT, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-053	Command and Control - FIN7, POWERPLANT, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-054	Command and Control - FIN7, POWERPLANT, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-055	Command and Control - FIN7, POWERPLANT, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-059	Command and Control - FOWLGAZE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-060	Command and Control - FOWLGAZE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-061	Command and Control - FOWLGAZE, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-062	Command and Control - FOWLGAZE, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-063	Command and Control - FOWLGAZE, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-064	Command and Control - FOWLGAZE, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-210	Command and Control - APT29, QUIETEXIT, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-215	Command and Control - UNC2824, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-259	Command and Control - APT29, QUIETEXIT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-260	Command and Control - APT29, QUIETEXIT, DNS Query, Variant #2	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-261	Command and Control - APT29, QUIETEXIT, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-343	Command and Control - ASYNCRAT, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-348	Command and Control - AZORULT, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A103-349	Command and Control - AZORULT, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A103-350	Command and Control - AZORULT, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A103-351	Command and Control - URSNIF, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-354	Command and Control - REMCOS, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-357	Command and Control - NANOCORE, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-359	Command and Control - AGENTTESLA, DNS Query, Variant #17	Content no longer meets Validation's standards of use
A103-360	Command and Control - NANOCORE, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-362	Command and Control - NANOCORE, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-364	Command and Control - LOKIBOT, DNS Query, Variant #11	Content no longer meets Validation's standards of use
A103-366	Command and Control - LOKIBOT, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A103-372	Command and Control - LOKIBOT, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A103-375	Command and Control - EMOTET, DNS Query, Variant #21	Content no longer meets Validation's standards of use
A103-376	Command and Control - EMOTET, DNS Query, Variant #20	Content no longer meets Validation's standards of use
A103-377	Command and Control - EMOTET, DNS Query, Variant #19	Content no longer meets Validation's standards of use
A103-378	Command and Control - EMOTET, DNS Query, Variant #18	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-379	Command and Control - EMOTET, DNS Query, Variant #22	Content no longer meets Validation's standards of use
A103-385	Command and Control - HELLOBOT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-387	Command and Control - JRAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-389	Command and Control - VERBLECON, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-414	Command and Control - Team 338, BOZOK, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-417	Command and Control - Team 338, BUBBLEWRAP, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-418	Command and Control - Team 338, BUBBLEWRAP, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-421	Command and Control - Team 338, BUBBLEWRAP, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-423	Command and Control - Team 338, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-424	Command and Control - Team 338, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-425	Command and Control - Team 338, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-426	Command and Control - Team 338, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-427	Command and Control - Team 338, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-428	Command and Control - Team 338, POISONIVY, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-429	Command and Control - Team 338, POISONIVY, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-430	Command and Control - Team 338, POISONIVY, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-432	Command and Control - Team 338, POISONIVY, DNS Query, Variant #4	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-435	Command and Control - UNC2500, LOKIBOT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-436	Command and Control - UNC2500, NUTWAFFLE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-437	Command and Control - UNC2500, NUTWAFFLE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-438	Command and Control - UNC2500, NUTWAFFLE, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-440	Command and Control - UNC2500, QAKBOT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-494	Command and Control - APT42, GHAMBAR, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-497	Command and Control - UNC2078, JSOUTPROX, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-498	Command and Control - UNC2078, JSOUTPROX, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-499	Command and Control - UNC2078, JSOUTPROX, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-501	Command and Control - UNC2078, JSOUTPROX, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-502	Command and Control - UNC2078, JSOUTPROX, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-534	Command and Control - APT43.SMART, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-535	Command and Control - APT43.SMART, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-539	Command and Control - APT43.SMART, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-540	Command and Control - APT43.SMART, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-547	Command and Control - UNC2922, PUFFPASTRY, DNS Query, Variant #2	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-548	Command and Control - UNC2922, PUFFPASTRY, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-550	Command and Control - UNC2922, PUFFPASTRY, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-562	Command and Control - UNC2565, GOOTLOADER, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-563	Command and Control - UNC2565, GOOTLOADER, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-564	Command and Control - UNC2565, GOOTLOADER, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-566	Command and Control - UNC2565, GOOTLOADER, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-567	Command and Control - ASYNCRAT, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-568	Command and Control - ASYNCRAT, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-569	Command and Control - ASYNCRAT, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-574	Command and Control - UNC3840, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-575	Command and Control - UNC3840, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-577	Command and Control - UNC2165, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-578	Command and Control - UNC2165, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-579	Command and Control - UNC2165, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-580	Command and Control - UNC2165, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-581	Command and Control - UNC2165, DNS Query, Variant #5	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-582	Command and Control - UNC2165, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-583	Command and Control - UNC2165, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A103-584	Command and Control - UNC2165, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A103-627	Command and Control - BEACON, SHELLSTING, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-628	Command and Control - BEACON, SHELLSTING, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-629	Command and Control - UNC3658, HTCLIENT.V2, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-687	Command and Control - APT29, ROOTSAW, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-705	Command and Control - UNC215, HYPERBRO, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-708	Command and Control - UNC215, QUICKBALL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-724	Command and Control - UNC215, FOCUSFJORD, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-732	Command and Control - TEMP.Armageddon, BADBORSCH, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-733	Command and Control - TEMP.Armageddon, BADBORSCH, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-744	Command and Control - FIN11, FRIENDSHOUT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-745	Command and Control - FIN11, FRIENDSHOUT, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-746	Command and Control - FIN11, FRIENDSHOUT, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-748	Command and Control - TEMP.Armageddon, PLAYDATE, DNS Query, Variant #1	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-749	Command and Control - TEMP.Armageddon, PLAYDATE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-750	Command and Control - TEMP.Armageddon, PLAYDATE, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-751	Command and Control - TEMP.Armageddon, PLAYDATE, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-752	Command and Control - UNC1189, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-753	Command and Control - UNC1189, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-754	Command and Control - UNC1189, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-755	Command and Control - UNC1189, EMPIRE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-756	Command and Control - UNC1189, PIECEMEAL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-757	Command and Control - UNC1189, PIECEMEAL, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-758	Command and Control - UNC1189, PIECEMEAL, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-759	Command and Control - UNC1189, PIECEMEAL, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-760	Command and Control - UNC1189, PIECEMEAL, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-815	Command and Control - UNC2743, STONEDOWN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-819	Command and Control - UNC2743, STONEDOWN, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-823	Command and Control - UNC1344, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-827	Command and Control - GH0ST, DNS Query, Variant #2	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-831	Command and Control - POISONIVY, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-832	Command and Control - UNC2420, REDISLAND, DNS Query, Variant #11	Content no longer meets Validation's standards of use
A103-833	Command and Control - REDISLAND, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-834	Command and Control - REDISLAND, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-835	Command and Control - REDISLAND, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-836	Command and Control - REDISLAND, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-837	Command and Control - REDISLAND, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-838	Command and Control - REDISLAND, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A103-840	Command and Control - REDISLAND, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A103-841	Command and Control - REDISLAND, DNS Query, Variant #11	Content no longer meets Validation's standards of use
A103-843	Command and Control - REDISLAND, DNS Query, Variant #13	Content no longer meets Validation's standards of use
A103-844	Command and Control - REDISLAND, DNS Query, Variant #14	Content no longer meets Validation's standards of use
A103-845	Command and Control - SOGU, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-846	Command and Control - SOGU, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-847	Command and Control - SOGU, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-848	Command and Control - UNC2420, REDISLAND, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-849	Command and Control - UNC2420, REDISLAND, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-852	Command and Control - UNC2420, REDISLAND, DNS Query, Variant #5	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-853	Command and Control - UNC2420, REDISLAND, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A103-854	Command and Control - UNC2420, REDISLAND, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A103-855	Command and Control - UNC2420, REDISLAND, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A103-856	Command and Control - UNC2420, REDISLAND, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A103-924	Command and Control - APT41, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-925	Command and Control - REDISLAND, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A103-926	Command and Control - UNC2420, REDISLAND, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-951	Command and Control - MATANBUCHUS, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-952	Command and Control - TEMP.Armageddon, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-955	Command and Control - TEMP.Armageddon, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A103-956	Command and Control - TEMP.Armageddon, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A103-957	Command and Control - TEMP.Armageddon, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-958	Command and Control - TEMP.Armageddon, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A103-959	Command and Control - TEMP.Armageddon, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A103-977	Command and Control - DARKTACO, DNS Query, Variant #1	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A103-979	Command and Control - UNC2589, SPRINGBEE, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-983	Command and Control - APT29, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A103-997	Command and Control - APT29, BEACON, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A103-998	Command and Control - APT29, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-221	Command and Control - APT29, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-224	Command and Control - UNC251, PUPYRAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-225	Command and Control - UNC251, HELLOBOT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-226	Command and Control - UNC251, HELLOBOT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-227	Command and Control - UNC94, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-231	Command and Control - UNC94, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-232	Command and Control - UNC94, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-250	Command and Control - UNC3661, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-254	Command and Control - UNC3661, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-296	Command and Control - APT42, TABBYCAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-311	Command and Control - APT28, DARKCRYSTALRAT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-312	Command and Control - APT44, DARKCRYSTALRAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-317	Command and Control - APT34, WEBPIPE, DNS Query, Variant #1	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A105-318	Command and Control - APT34, WEBPIPE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-319	Command and Control - APT34, WEBPIPE, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-322	Command and Control - UNC3443, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-323	Command and Control - UNC3443, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-324	Command and Control - UNC3443, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A105-326	Command and Control - UNC3443, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A105-384	Command and Control - APT42, PINEFLOWER, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-385	Command and Control - APT42, PINEFLOWER, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-393	Command and Control - DOUBLEPIPE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-394	Command and Control - PEARLDOWN Dropper, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-395	Command and Control - PEARLDOWN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-396	Command and Control - PEARLDOWN, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-401	Command and Control - Tonto Team, CALMTHORN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-402	Command and Control - Tonto Team, CALMTHORN, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-403	Command and Control - Tonto Team, CALMTHORN, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-404	Command and Control - Tonto Team, CALMTHORN, DNS Query, Variant #4	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A105-405	Command and Control - UNC3840, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-407	Command and Control - APT44, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-408	Command and Control - APT44, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-453	Command and Control - Tonto Team, DOUBLEPIPE, CALMTHORN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-483	Command and Control - UNC776, PLANEPATCH, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-484	Command and Control - UNC776, PLANEPATCH, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-532	Command and Control - UNC3944, REMCOS, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-533	Command and Control - UNC3944, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-536	Command and Control - UNC3944, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-553	Command and Control - UNC3443, DNS Query, Variant #11	Content no longer meets Validation's standards of use
A105-558	Command and Control - SNOWCONE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-562	Command and Control - UNC3443, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A105-565	Command and Control - UNC3443, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A105-566	Command and Control - UNC3443, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A105-577	Command and Control - UNC757, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-586	Command and Control - UNC2628, BEACON, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-587	Command and Control - UNC2628, BEACON, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-588	Command and Control - UNC2628, BEACON, DNS Query, Variant #3	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A105-590	Command and Control - UNC2628, DARKSIDE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-591	Command and Control - UNC2628, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-592	Command and Control - UNC2628, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-593	Command and Control - UNC638.GILG, ANDROMEDA, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-594	Command and Control - UNC638.GILG, ANDROMEDA, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-645	Command and Control - UNC94, FRONTPORCH, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-646	Command and Control - UNC94, TEMPFUN, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-647	Command and Control - UNC94, TEMPFUN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-648	Command and Control - UNC94, TEMPFUN, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-649	Command and Control - UNC94, FRONTPORCH, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-650	Command and Control - UNC94, FRONTPORCH, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-651	Command and Control - UNC94, HERBDOOR, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-653	Command and Control - UNC94, TEMPFUN, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-655	Command and Control - UNC94, FRONTPORCH, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-716	Command and Control - JUMPLUMP, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-718	Command and Control - KNOTWEED, DNS Query, Variant #2	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A105-720	Command and Control - KNOTWEED, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-724	Command and Control - BATLOADER, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-725	Command and Control - BATLOADER, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-726	Command and Control - BATLOADER, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A105-729	Command and Control - BATLOADER, DNS Query, Variant #15	Content no longer meets Validation's standards of use
A105-730	Command and Control - BATLOADER, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A105-733	Command and Control - BATLOADER, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-734	Command and Control - BATLOADER, DNS Query, Variant #17	Content no longer meets Validation's standards of use
A105-735	Command and Control - BATLOADER, DNS Query, Variant #18	Content no longer meets Validation's standards of use
A105-736	Command and Control - BATLOADER, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A105-737	Command and Control - BATLOADER, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A105-738	Command and Control - BATLOADER, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A105-741	Command and Control - QAKBOT, DNS Query, Variant #11	Content no longer meets Validation's standards of use
A105-743	Command and Control - QAKBOT, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A105-744	Command and Control - QAKBOT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-746	Command and Control - QAKBOT, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A105-747	Command and Control - QAKBOT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-748	Command and Control - QAKBOT, DNS Query, Variant #6	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A105-749	Command and Control - QAKBOT, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A105-750	Command and Control - QAKBOT, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A105-751	Command and Control - QAKBOT, DNS Query, Variant #12	Content no longer meets Validation's standards of use
A105-752	Command and Control - QAKBOT, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A105-753	Command and Control - QAKBOT, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-754	Command and Control - QAKBOT, DNS Query, Variant #14	Content no longer meets Validation's standards of use
A105-755	Command and Control - QAKBOT, DNS Query, Variant #13	Content no longer meets Validation's standards of use
A105-756	Command and Control - QAKBOT, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-758	Command and Control - TEMP.Armageddon, ROSEHILL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-769	Command and Control - XCODESPY, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-777	Command and Control - XCODESPY, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-779	Command and Control - UNC4322, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-786	Command and Control - UNC2589, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-787	Command and Control - UNC2589, SPRINGBEE, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A105-791	Command and Control - UNC2589, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-793	Command and Control - UNC3808, ANGRYREBEL.LINUX, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-829	Command and Control - APT43, BITTERSWEET, DNS Query, Variant #1	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A105-836	Command and Control - APT43, PENCILDOWN.ANDROID, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-837	Command and Control - APT43, PENCILDOWN.ANDROID, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-839	Command and Control - APT43, DRIVEDOWN, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-840	Command and Control - APT43, DRIVEDOWN, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-843	Command and Control - APT43, DRIVEDOWN, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-854	Command and Control - APT43, QUIBBLEDOWN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-855	Command and Control - APT43, QUIBBLEDOWN, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-863	Command and Control - APT43, GIANTDIME, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-864	Command and Control - APT43, GIANTDIME, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-865	Command and Control - APT43, GIANTDIME, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-866	Command and Control - APT43, GIANTDIME, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-879	Command and Control - APT43, LOGCABIN, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-882	Command and Control - APT43, TROIBOMB, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-884	Command and Control - APT43, TROIBOMB, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-885	Command and Control - APT43, TROIBOMB, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-886	Command and Control - APT43, TROIBOMB, DNS Query, Variant #5	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A105-887	Command and Control - APT43, TROIBOMB, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A105-891	Command and Control - APT43, GOLDDRAGON, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-892	Command and Control - APT43, GOLDDRAGON, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-893	Command and Control - APT43, GOLDDRAGON, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-894	Command and Control - APT43, GOLDDRAGON, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-895	Command and Control - APT43, GOLDDRAGON.POWERSHELL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-909	Command and Control - APT43, COINTOSS, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-911	Command and Control - APT43, COINTOSS, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-912	Command and Control - APT43, COINTOSS, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A105-913	Command and Control - APT43, COINTOSS, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-914	Command and Control - APT43, COINTOSS.XLM, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-915	Command and Control - APT43, COINTOSS.XLM, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-917	Command and Control - APT43, COINTOSS.XLM, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A105-935	Command and Control - APT43, PENCILDOWN, DNS Query, Variant #1	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A105-941	Command and Control - APT43, HANGMAN.V2, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-969	Command and Control - APT43, LATEOP, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-971	Command and Control - APT43, JURASSICSHELL, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-987	Command and Control - FIN6, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-995	Command and Control - FIN11, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A105-996	Command and Control - FIN11, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A105-997	Command and Control - FIN11, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-007	Command and Control - SNOWCONE.GZIPLOADER, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-015	Command and Control - UNC2926, UNC2420, UNC3151, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-017	Command and Control - SNOWCONE.GZIPLOADER, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-042	Command and Control - TEMP.Hex, SOGU, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-065	Command and Control - SAITAMA, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-066	Command and Control - SAITAMA, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-072	Command and Control - SAITAMA, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-089	Command and Control - DNS Query, webdavml07[.]bplaced[.]net	Content no longer meets Validation's standards of use
A106-091	Command and Control - DNS Query, st-g[.]server-panel[.]net	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-102	Command and Control - APT44, QUICKTOW, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-106	Command and Control - APT44, GOGETTER, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-108	Command and Control - VIDAR, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-115	Command and Control - URSNIF, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A106-124	Command and Control - URSNIF, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A106-125	Command and Control - URSNIF, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A106-128	Command and Control - URSNIF, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A106-130	Command and Control - BRC4, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-143	Command and Control - UNC3890, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-144	Command and Control - UNC3890, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-152	Command and Control - UNC3890, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-157	Command and Control - APT43, JURASSICSHELL, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-170	Command and Control - APT29, ROOTSAW, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-182	Command and Control - UNC2500, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-185	Command and Control - UNC2500, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-188	Command and Control - APT44, BRUSHPASS, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-208	Command and Control - UNC215.VALENTINA, BLACKASINO, DNS Query, Variant #1	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-210	Command and Control - UNC215.VALENTINA, BLACKASINO, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-211	Command and Control - UNC215.VALENTINA, BLACKASINO, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-214	Command and Control - UNC215.VALENTINA, BLACKASINO, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A106-217	Command and Control - UNC215.VALENTINA, BLACKASINO, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-218	Command and Control - UNC215.VALENTINA, BLACKASINO, FRESHLIME, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-241	Command and Control - UNC1530, SADPIZZA, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-250	Command and Control - UNC1530, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-251	Command and Control - UNC1530, GREASYPIZZA, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-252	Command and Control - UNC1530, SADPIZZA, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-253	Command and Control - UNC1530, SADPIZZA, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-255	Command and Control - UNC1530, SADPIZZA, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-258	Command and Control - UNC1530, SHARKPIZZA, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-262	Command and Control - UNC1530, SUPERSPEED, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-275	Command and Control - LOADINFO, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-296	Command and Control - CVE-2022-0609, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-297	Command and Control - CVE-2022-0609, DNS Query, Variant #3	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-298	Command and Control - CVE-2022-0609, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-299	Command and Control - CVE-2022-0609, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-300	Command and Control - CVE-2022-0609, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A106-302	Command and Control - DADSTACHE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-303	Command and Control - DADSTACHE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-316	Command and Control - TEMP.Hermit, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-319	Command and Control - UNC4736, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-321	Command and Control - UNC4736, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-323	Command and Control - UNC4736, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-392	Command and Control - BEACON, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A106-394	Command and Control - BEACON, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A106-397	Command and Control - BEACON, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-398	Command and Control - BEACON, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A106-400	Command and Control - UNC2900, BEACON, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-402	Command and Control - UNC2900, BEACON, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-403	Command and Control - UNC2900, BEACON, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-409	Command and Control - UNC4742, CRABWISE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-416	Command and Control - TEMP.Hex, DNS Query, Variant #8	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-450	Command and Control - TEMP.Scimitar, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-451	Command and Control - TEMP.Scimitar, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-452	Command and Control - TEMP.Scimitar, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-463	Command and Control - UNC4841, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-475	Command and Control - REDHAWK.V2, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-479	Command and Control - UNC1543, FAKEUPDATES, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-485	Command and Control - UNC1819, COLDPOT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-486	Command and Control - UNC1819, CLUBHOUSE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-501	Command and Control - TEMP.Tick, TRIPMISS, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-508	Command and Control - UNC3443, DNS Query, Variant #16	Content no longer meets Validation's standards of use
A106-509	Command and Control - UNC3443, DNS Query, Variant #15	Content no longer meets Validation's standards of use
A106-510	Command and Control - UNC3443, DNS Query, Variant #13	Content no longer meets Validation's standards of use
A106-512	Command and Control - UNC3443, DNS Query, Variant #14	Content no longer meets Validation's standards of use
A106-542	Command and Control - APT29, MUSKYBEAT , DNS Query	Content no longer meets Validation's standards of use
A106-577	Command and Control - GRAYRABBIT, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-578	Command and Control - GRAYRABBIT, DNS Query, Variant #1	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-586	Command and Control - BEACON, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-587	Command and Control - UNC4899, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-588	Command and Control - UNC4899, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-589	Command and Control - UNC4899, STRATOFEAR, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-590	Command and Control - UNC4899, TIEDYE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-591	Command and Control - UNC4899, TIEDYE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-592	Command and Control - UNC4899, STRATOFEAR, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-618	Command and Control - UNC2554, POOLRAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-619	Command and Control - POOLRAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-620	Command and Control - UNC4736, POOLRAT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-624	Command and Control - UNC4351, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-626	Command and Control - UNC4351, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-628	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A106-642	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-643	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-645	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #4	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-650	Command and Control - UNC4814, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-659	Command and Control - TEMP.Hex, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A106-663	Command and Control - UNC4351, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-664	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-666	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A106-667	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A106-685	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A106-686	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #12	Content no longer meets Validation's standards of use
A106-687	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #11	Content no longer meets Validation's standards of use
A106-688	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #13	Content no longer meets Validation's standards of use
A106-691	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A106-693	Command and Control - UNC4814, SMOKELOADER, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A106-700	Command and Control - SPLITPUSH, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-701	Command and Control - SPLITPUSH, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-709	Command and Control - UNC4841, DNS Query, Variant #10	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-710	Command and Control - UNC4841, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-711	Command and Control - UNC4841, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-712	Command and Control - UNC4841, DNS Query, Variant #11	Content no longer meets Validation's standards of use
A106-713	Command and Control - UNC4841, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-714	Command and Control - UNC4841, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A106-715	Command and Control - UNC4841, DNS Query, Variant #8	Content no longer meets Validation's standards of use
A106-716	Command and Control - UNC4841, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A106-717	Command and Control - UNC4841, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A106-718	Command and Control - UNC4841, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A106-723	Command and Control - UNC3707, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-724	Command and Control - UNC3707, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-725	Command and Control - UNC3707, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-728	Command and Control - UNC4221, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A106-729	Command and Control - UNC4221, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-730	Command and Control - UNC4221, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A106-731	Command and Control - UNC4221, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-732	Command and Control - UNC4221, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-733	Command and Control - UNC4221, DNS Query, Variant #7	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-734	Command and Control - UNC4221, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-737	Command and Control - UNC4984, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-738	Command and Control - UNC4984, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-740	Command and Control - UNC4812, SIMPLELOADER, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-748	Command and Control - URSNIF, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A106-749	Command and Control - URSNIF, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A106-762	Command and Control - UNC3507, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-781	Command and Control - UNC2975, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-782	Command and Control - UNC2975, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-784	Command and Control - UNC2975, PAPERDROP, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-790	Command and Control - UNC1151, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-791	Command and Control - UNC1151, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-799	Command and Control - UNC1151, BEACON, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-806	Command and Control - Molerats, Malicious Executable, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-807	Command and Control - Molerats, BLACKBELT, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-808	Command and Control - SPYNOTE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-810	Command and Control - UNC718, WHITEWALK, DNS Query, Variant #2	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-811	Command and Control - THREESECRET, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-812	Command and Control - UNC718, WHITEWALK, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-826	Command and Control - Molerats, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-872	Command and Control - UNC2975, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A106-873	Command and Control - UNC2975, DNS Query, Variant #6	Content no longer meets Validation's standards of use
A106-874	Command and Control - UNC2975, DNS Query, Variant #9	Content no longer meets Validation's standards of use
A106-882	Command and Control - UNC2975, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A106-884	Command and Control - UNC2975, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-886	Command and Control - UNC2975, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A106-890	Command and Control - UNC2975, DNS Query, Variant #10	Content no longer meets Validation's standards of use
A106-894	Command and Control - UNC4536, NUMOZYLOD, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-898	Command and Control - UNC4990, EMPTYSPACE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-903	Command and Control - UNC4536, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-907	Command and Control - UNC4536, NUMOZYLOD, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-928	Command and Control - UNC5092, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-933	Command and Control - UNC5225, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-941	Command and Control - WARPWIRE, DNS Query, Variant #3	Content no longer meets Validation's standards of use

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
A106-942	Command and Control - WARPWIRE, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-944	Command and Control - WARPWIRE, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-956	Command and Control - UNC4536, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A106-960	Command and Control - UNC5101, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-966	Command and Control - UNC3319, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A106-971	Command and Control - UNC4536, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A106-973	Command and Control - UNC4536, NUMOZYLOD, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A107-087	Command and Control - UNC2926, DNS Query, Variant #4	Content no longer meets Validation's standards of use
A107-088	Command and Control - SNOWCONE.GZIPLOADER, DNS Query, Variant #5	Content no longer meets Validation's standards of use
A107-089	Command and Control - UN2926, DNS Query, Variant #2	Content no longer meets Validation's standards of use
A107-091	Command and Control - UNC2926, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A107-093	Command and Control - TEMP.Armageddon, DNS Query, Variant #7	Content no longer meets Validation's standards of use
A107-099	Command and Control - UNC2926, DNS Query, Variant #3	Content no longer meets Validation's standards of use
A107-105	Command and Control - UNC4984, SIMPLELOADER, DNS Query, Variant #1	Content no longer meets Validation's standards of use
A107-213	Command and Control - SNOWLIGHT, DNS Query, Variant #1	Content no longer meets Validation's standards of use

Sequences

VID	Name	Reason for Removal

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Reason for Removal
S100-103	Malicious Activity Scenario - LOCKERGOGA Ransomware Infection	Content no longer meets Validation's standards of use
S100-113	Malicious Activity Scenario - LOKIBOT Malware Infection	Content no longer meets Validation's standards of use
S100-226	Malicious Activity Scenario - Campaign 22-048, UNC4300 Gains Access via Initial Access Operator UNC2633	Content no longer meets Validation's standards of use
S100-240	Malicious Activity Scenario - APT43, BENCHMARK Leveraged Against Government Entities	Content no longer meets Validation's standards of use
S100-263	Malicious Activity Scenario - Campaign 23-006, UNC2500 Distributing QAKBOT via OneNote File in Phishing Campaign	Content no longer meets Validation's standards of use

Evaluations

VID	Name	Reason for Removal
S100-071	Evaluation: APT28/SOFACY/FANCY BEAR Activity	Content no longer meets Validation's standards of use
S100-101	Evaluation: THE DARK OVERLOAD	Content no longer meets Validation's standards of use
S100-176	Evaluation: UNC3004	Content no longer meets Validation's standards of use
S100-177	Evaluation: UNC2452	Content no longer meets Validation's standards of use
S100-180	Evaluation: UNC2652	Content no longer meets Validation's standards of use
S100-276	Evaluation: APT27	Content no longer meets Validation's standards of use
S100-912	Benign Actions for VoD Actor - Endpoint Based Actions	Content no longer meets Validation's standards of use
S100-913	Benign Actions for VoD Actor: Network Based Actions	Content no longer meets Validation's standards of use

Updated Content

Changes include improved consistency in execution, description details, and tags. For more information, see **Content pack downloads (https://docs.mandiant.com/home/msv-content-packs)** (requires sign in).

Supported Operating Systems (OS) and Platforms

VRT used the following environments to test the Validation content included in this update. Each Action is assigned OS/Platform Tags, which you can see when viewing the Action in the Action Library. These tags indicate which environments we expect the Action to run successfully on and are the environments the Actions were tested on.

Mandiant Security Validation Platform

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

System	Build Number / Version
Director	4.14.4.1-51
Actor	4.12.4.1-8

Endpoint Actions

OS/Platform	Common Platform Enumeration (CPE)
Windows 11	cpe:2.3:o:microsoft:windows_11:22000:*:*:en-us:*:*:x64
Windows 10	cpe:2.3:o:microsoft:windows_10:19041:*:*:en-us:*:*:x64
Windows Server 2019	cpe:2.3:o:microsoft:windows_server_2019:17763:*:*:en-us:*:*:x64
Windows Server 2016	cpe:2.3:o:microsoft:windows_server_2016:14393:*:*:en-us:*:*:x64
Linux: Ubuntu	cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:en-us:*:*:x64
Linux: CentOS	cpe:2.3:o:redhat:enterprise_linux:7.8:*:*:en-us:*:*:x64
macOS	cpe:2.3:o:apple:macosx:11.5.2:*:*:en-us:*:*:x64

Network Actions

OS/Platform	Common Platform Enumeration (CPE)
Linux: CentOS	cpe:2.3:o:redhat:enterprise_linux:7.8:*:*:en-us:*:*:x64

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.