TREND MICRO | research

Exposing Modular Adware: How DealPly, IsErIk, and ManageX Persist in Systems

Appendix

By RonJay Caragay, Fe Cureg, Ian Lagrazon, Erika Mendoza, and Jay Yaneza

Observed domain names

Browser extension

Boqudo[.]com

Bujot[.]com

Cabarula[.]com

Cunakod[.]com

Focuquc[.]com

Gapoloha[.]com

Gasasot[.]com

Jafuq[.]com

Juronu[.]com

Norugu[.]com

Nusojog[.]com

Pacudoh[.]com

Pudacasa[.]com

Qaloqum[.]com

Qamopo[.]com

Qukusut[.]com

Rokuq[.]com

Sastts[.]com

Tawuhoju[.]com

Tocopada[.]com

Toluhuku[.]com

Fileless execution (wscript)

hxxps://busucak[.]com

hxxps://butapujo[.]com

hxxps://d1etigj2h443kd[.]cloudfront[.]net

hxxps://d1hpofzsaxmzog[.]cloudfront[.]net

hxxps://d274eq41c39r2n[.]cloudfront[.]net

hxxps://d2b46e7ax2atfi[.]cloudfront[.]net

hxxps://d2vut1jfnnygcg[.]cloudfront[.]net

hxxps://d2wv7denc1jx9z[.]cloudfront[.]net

hxxps://d2zyvlskj53q65[.]cloudfront[.]net

hxxps://d33wv995bk7lag[.]cloudfront[.]net

hxxps://d36lv9781gxp5z[.]cloudfront[.]net

hxxps://d3s1tkg9f4254q[.]cloudfront[.]net

hxxps://d3tq9gtc0bxu1s[.]cloudfront[.]net

hxxp://ddukmql[.]com

hxxps://ddukmql[.]com

hxxps://dlrabaly59cp3[.]cloudfront[.]net

hxxps://dnodjoiz0vcnz[.]cloudfront[.]net

hxxps://gahuwa[.]com

hxxps://gujujoh[.]com

hxxps://hoduqoq[.]com

hxxps://hufunuk[.]com

hxxps://katunaq[.]com

hxxps://lomokonu[.]com

hxxps://mogaf[.]com

hxxps://pugugu[.]com

hxxp://puloja[.]com

hxxps://puloja[.]com

hxxp://sao[.]kanrq[.]com

hxxps://qajolos[.]com

hxxps://rududulu[.]com

hxxp://tdfpa[.]com

hxxps://tdfpa[.]com

hxxp://wagng[.]com

hxxps://wagng[.]com

hxxp://wavbsly[.]com

hxxps://wavbsly[.]com

hxxp://yxhpa[.]com

hxxps://yxhpa[.]com

hxxp://zahirq[.]com

From DealPly binaries

Adofd[.]com

Buluw[.]com

Bxvdc[.]com

Daqah[.]com

Eakqz[.]com

Fotuwuk[.]com

Gukacado[.]com

Hahofaba[.]com

Hajanac[.]com

Kugocu[.]com

Nutojo[.]com

Pajuwu[.]com

Pawotapu[.]com

Pocxc[.]com

Pofufaco[.]com

Ruqut[.]com

Sanupu[.]com

Suhacuc[.]com

Tomupaj[.]com

Tuwoqol[.]com

Tuwoqol[.]com

Uyvsa[.]com

Wugulaf[.]com

Browser extension AppID related to MANAGEX

Bifdhahddjbdbjmiekcnmeiffabcfjgh

nabmpeienmkmicpjckkgihobgleppbkc

bgbeocleofdgkldamjapfgcglnmhmjgb

ncjbeingokdeimlmolagjaddccfdlkbd

jghiljaagglmcdeopnjkfhcikjnddhhc

Note: Abovementioned lists are only some of the indicators we encountered in our analyses; the different adware have more indicators as they develop.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com