CMC cảnh báo chiến dịch APT đang tấn công vào các cơ quan hành chính Nhà nước Việt Nam.

Công ty CMC Cyber Security ã có nhng phân tích sâu v nhng file mã c c s dng trong chin dch tn công này. Qua quá trình tìm hiu và phân tích các du hiu, mu mã c phc v cho cuc tn công này, các chuyên gia phân tích mã c ca CMC Cyber Security nhn nh nhóm tn công có kh nng bt ngun t Trung Quc. C th, chuyên gia xác nh c các vn bn c hi tn công vào Vit Nam trong chin dch này bt ngun t nhóm Mustang Panda, mt nhóm tin tc c ánh giá rt cao bi nhng chin dch rt bài bn, có k thut và chin thut c bit.

Các mu nhn c sau khi phân tích có th chia làm hai loi. Mi loi s dng mt cách thc thi payload khác nhau nhng vn có mt s c im chung sau: Các sample c gi ti nn nhân c nén trong file zip tránh b chn bi các ng dng. Trong file nén có cha file shortcut .lnk kèm theo uôi .doc(ví d sample.doc.lnk) ánh la ngi dùng. File lnk ính kèm theo file hta có th thc thi c script. Script m file document ính kèm cho ngi dùng và ngm thc thi payload.

Vi loi th nht, mu là mt file shortcut có phn m rng uôi là .lnk, thng c t tên kèm theo uôi .doc ánh la ngi dùng do uôi .lnk s c Windows n i. im áng ng là phn target ca file shortcut. Tuy nhiên, target ca mu cha mt on command khi chy tin trình Mshta.exe thc thi file hta nhúng kèm. Khi ngi dùng m file lnk, máy s thc thi command trong target ca file lnk và thc thi file mshta.exe m chính nó.

Tng t nh loi mt, loi hai cng là mt file lnk c nhúng vào trc file hta. giai on thc thi vbscript, on script trong malware s gii mã và lu vào th mc %temp% 2 file binary, 1 file là payload và 1 file document hin th cho ngi dùng.

Dữ liệu người đã bị hacker tấn công.

Mc ích ca tt các các mu thu thp c u là connect n c&c server, download các mã c nhm ánh cp thông

tin ngi dùng và cung cp chc nng iu khin máy t xa.

iu áng nói nht là tinh xo trong các file tài liu c to ra nhm ánh la ngi dùng. Khác vi nhng mu AP ta phi i mt mt vài nm trc, tài liu “mi” c vit rt cu th, câu cú lng cng, tài liu chp vá vi hình thc không phù hp vi vn bn chính quy thì gn ây, chính xác và t m trong các vn bn tn công rt d la c ngi dùng. c bit ngay c trong ni dung, vn bn cng c th hin rõ mc ích chính tr.

Trc vic ngn chn toàn din chin dch tn công APT rt khó khn, các chuyên gia ca CMC Cyber Security a ra khuyn cáo cho khách hàng các bin pháp ngn nga, gim thiu và phát hin sm các tác hi ca tn công APT.

i vi ngi dùng hãy cn trng khi tip nhn email, ng link, tp tin l; xác thc chính xác ngun gi an toàn, áng tin cy; s dng các công c Endpoint Security.

i vi doanh nghip nên trin khai các h thng giám sát, phát hin hoc ngn chn xâm nhp trái phép; nh k ánh giá, kim nh các mi nguy hi i vi h thng. Doanh nghip cn nâng cao nhn thc ca tng cá nhân trong tp th v tránh nhim m bo an ninh, an toàn thông tin và có k hoch ng phó vi s c.

Hin nay CMC Cyber Security ã có phn mm chuyên bit dành cho mã c mã hoá d liu bn mi nht ca CMC Antivirus/CMC Internet Security, ngi dùng cá nhân có th cài phn mm chng virus trên di ng và máy tính ngn chn kp thi trc khi máy tính b lây nhim.

APT là tên vit tt ca Advanced Persistent Threat - thut ng rng dùng mô t mt chin dch tn công, thng do mt nhóm các k tn công, s dng nhng k thut tn công nâng cao có th hin din và tn ti lâu dài trên mng Internet nhm khai thác d liu có nhy cm cao.

PV

(Theo: Trang thông tin điện tử tổng hợp ICTNews – Ngày đưa tin: 28/10/2019)