Ransomware-taldea: Agent Tesla

Laburpen exekutiboa

Agent Tesla *Remote Access Trojan* (RAT) eta ***infostealer*** aktiboa da 2014az geroztik, ***malware-as-a-service*** (MaaS) ereduaren bidez banatua, ziberkrimen-kanpainetan asko erabiltzen dena. Agent Tesla Espainian gehien detektatutako mehatxuetako bat da, **konprometitutako ekipoen informazioa lapurtzeko eta kredentzialak esfiltratzeko duen gaitasunagatik.** Malwarea, batez ere, **phishing kanpainen** bidez hedatzen da, ondoren *payloada* deskargatzen duten eranskin kaltegarriekin edo dokumentuekin.

Behin instalatuta, Agent Teslak **lausotze- eta iraunkortasun-teknikak** erabiltzen ditu, eta nabigatzaileen, posta-bezeroen, VPNen eta aplikazio korporatiboen kredentzialen lapurretan espezializatuta dago. Gainera, bestelako funtzio batzuk ere baditu, hala nola ***keylogginga***, **pantaila-argazkiak** eta **arbelerako sarbidea**. Aldaera berrienek HTTP, SMTP eta FTP kanalak erabiltzen dituzte **esfiltrazio-metodoak** zabaltzeko; horri esker, lapurtutako informazioa erasotzaileek kontrolatutako zerbitzarietara bidal daiteke, modu malguagoan eta detektatzeko zailagoan.

Banaketa global zabala eta kredentzialak arriskuan jartzeko eta ondorengo sarbideak errazteko duen gaitasuna dela-eta, Agent Tesla **arrisku handia da sektore ugarietako antolakunde pribatuentzat, administrazio publikoarentzat eta herritarrentzat**.

Agent Tesla mehatxu **iraunkortzat** hartu behar da, **asko erabiltzen baita** informazioa lapurtzeko kanpainetan eta hasierako konpromiso-faseetan. Gomendatutako defentsek barne hartzen dute, besteak beste, **phishingaren aurkako babesa** indartzea, **MFA** hedatzea eta **EDR** konponbideak erabiltzea malwareari lotutako portaera anomaloak detektatzeko.

Ransomware-taldea: Agent Tesla

Agent Tesla RAT motako malwarea eta *infostealer* aktiboa da 2014az geroztik, MaaS gisa banatua. Malware hori monitorizazio-software “legitimo” gisa aurkezten den arren, haren dokumentazioak eta laguntza-materialek jarraibide esplizituak jasotzen dituzte antibirusak saihesteko eta kalteberatasunak ustiatzeko, eta horrek orientazio kriminal argia erakusten du. Eredu komertzial egituratua (MaaS), etengabeko bilakaera teknikoa eta erasotzaileentzako sarbide-hesi baxuak uztartzen dituenez, Agent Tesla mehatxu iraunkortzat hartu behar da.

Eragindako herrialdeak eta sektoreak

Agent Teslak **jarduera globala** mantendu du duela hamarkada bat baino gehiagotik, eta bere jarduera nagusia Europan, Asian eta Amerikan garatzen da.

Estatu mailan, malware horren jarduera apaldu egin zen 2024an, beste *infostealer* berriago batzuek neurri batean ordezkatu ondoren. Hala ere, malwareak aktibo jarraitzen du, 2025eko lehen hilabeteetan phishing-kanpainekin lotutako mezu kaltegarri ugari erregistratu baitziren, eta Agent Tesla berriro identifikatu zen banatutako *infostealer*-en artean.

Eragindako sektoreetan, Agent Tesla ez da industria espezifikoetara mugatzen; **hedapen masiboa du**. Hala ere, inpaktu handiena jasaten duten sektoreak izan ohi dira **kredentzial korporatiboak aktibo kritikoa diren** sektoreak, hala nola zerbitzu profesionalak, logistika, manufaktura, hezkuntza, teknologia eta administrazio publikoak. Gainera, enpresa txiki eta ertainek helburu ohikoenetako bat izaten jarraitzen dute, banaketa-kanpainen izaera indiskriminatua dela-eta.

Analisi teknikoa

Ikuspuntu tekniko batetik, Agent Tesla RAT eta infostealer bat da, nagusiki phishing bidez eranskin kaltegarriekin banatua. Exekutatu ondoren, bere egitura lausotzen du detekzioa saihesteko eta iraunkortasuna ezartzeko, sistema abiarazten den bakoitzean edo erabiltzaileak saioa hasten duen bakoitzean exekutatzen dela bermatuz.

Bilketa-fasean, sistema aztertzen du software espezifikoa eta kredentzial-biltegiak identifikatzeko. Gainera, hainbat funtzio aktibatzen ditu, hala nola *keyloggin*ga, pantaila-argazkiak eta arbelerako sarbidea.

Azkenik, datu-esfiltrazioa malgutasunez gauzatzen du, erasotzaileak konfiguratzeko moduko hainbat protokoloren bidez, hala nola HTTP, SMTP edo FTP. Zenbaitetan, TOR nabigatzailea erabiltzen du proxytzat, jarduera ezkutatzeko eta atribuzioa zailtzeko.

Ezaugarri tekniko nagusiak:

- **Mota eta plataforma**: .NETen idatzitako eta Windows sistemetarako diseinatutako RAT/infostealer
- **Banaketa-eredua:** Malware-as-a-Service (MaaS), ezkutuko foroetan saldua edo alokatua, aldizkako bertsio eta eguneratzeekin.
- **Ohiko infekzio-bektorea:** Phishing-mezuak, *payloada* deskargatzen edo abiarazten duten eranskin kaltegarriekin edo Office dokumentuekin.
- **Sistemaren informazioa biltzen du**: sistema eragilea, ekipoaren konfigurazioa, erabiltzaile-izena, IP publikoa, hardware-informazioa, etab.
- **Iraunkortasuna:** sisteman autoinstalatzeko gaitasuna, malwarea berrabiarazi ondoren bizirik dagoela eta ekipoan iraunkorra dela ziurtatuz.

MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
Initial Access	**T1566.001** — Phishing: Spearphishing Attachment
Execution	**T1053.005** — Scheduled Task/Job: Scheduled Task **T1203** — Exploitation for Client Execution **T1204.002** — User Execution: Malicious File **T1047** — Windows Management Instrumentation
Persistence	**T1547.001** — Registry Run Keys / Startup Folder **T1112** — Modify Registry
Privilege Escalation	**T1055** — Process Injection: Dynamic-link Library Injection **T1055.012** — Process Hollowing
Defense Evasion	**T1497** — Virtualization/Sandbox Evasion **T1218.009** — System Binary Proxy Execution: Regsvcs/Regasm **T1027** — Obfuscated Files or Information **T1564 —** Hidden Artifacts **T1140** — Deobfuscate/Decode Files or Information **T1562.001** — Impair Defenses: Disable or Modify Tools
Credential Access	**T1555** — Credentials from Password Stores
Discovery	**T1057** — Process Discovery **T1016** — System Network Configuration Discovery **T1082** — System Information Discovery **T1016.002** — Wi-Fi Discovery **T1033** — System Owner/User Discovery
Collection	**T1560** — Archive Collected Data **T1185** — Browser Session Hijacking **T1115** — Clipboard Data **T1056** — Input Capture: Keylogging **T1113** —Screen Capture
Command and Control	**T1071** — Application Layer Protocol **T1105** — Ingress Tool Transfer
Exfiltration	**T1048.003** — Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

Arintze-neurriak

Proaktiboak

- ❑ MFA inplementatzea kredentzial-lapurretaren eta baimendu gabeko sarbidearen inpaktua murrizteko. (T1555 - Credentials from Password Stores)
- ❑ Makroak blokeatzea eta eduki aktiboa desgaitzea posta elektronikotik datozen Office dokumentuetan. (T1203 - Exploitation for Client Execution)
- ❑ Baimendutako aplikazioen zerrendak aktibatzea (*allowlisting*), bitar ezezagunak exekutatzea eragozteko. (T1047 - Windows Management Instrumentation)
- ❑ Pribilegioak murriztea eta gutxieneko pribilegioen eredu bat aplikatzea, osagai kaltegarrien iraunkortasuna eta exekuzioa saihesteko. (T1562 - Impair Defenses)
- ❑ Kontzientziazioari buruzko etengabeko prestakuntza, bereziki mezu eta eranskin susmagarriak detektatzeko.(T1566.001 - Phishing: Spearphishing Attachment)

Erreaktiboak

- ❑ EDR edo antibirusak erabiltzea, keylogger-ak *eta fileless* jarduera detektatzeko gaitasuna dutenak, funtsezkoa azken aldaeren kasuan. (T1203 - Exploitation for Client Execution)
- ❑ Irteerako trafikoa monitorizatzea eta baimendu gabeko SMTP/FTP/HTTP konexioak blokeatzea, esfiltraziorako erabiltzen baitira. (T1048.003 - Exfiltration Over Unencrypted Non-C2 Protocol)

Ondorioak eta gomendioak

Agent Tesla *infostealer* **aktibo eta iraunkorra** da oraindik ere, nahiz eta bere presentzia murriztu den beste malware berri eta erasokorrago batzuen aldean. Hala ere, enpresa handiei zein ETEei eragiten dieten phishing-kanpainak aktibo mantentzen ditu, eta ***Malware-as-a-Service*** ereduak aukera ematen du sofistikazio-maila desberdineko eragileek hura ustiatzen jarraitzeko. Bere teknikek (kredentzialen lapurreta, *keyloggin*a, pantaila-argazkia, esfiltrazioa eta iraunkortasuna) **mehatxu garrantzitsu bihurtzen dute enpresa-sarearentzat, administrazio publikoarentzat zein herritarrentzat.**

Arriskua murrizteko, gomendatzen da postaren iragazketa aurreratua inplementatzea, makro eta artxibo kaltegarrien exekuzioa blokeatzea, sarbideak MFArekin indartzea eta erabiltzaile-pribilegioak mugatzea. Gainera, funtsezkoa da irteerako trafikoa monitorizatzea balizko esfiltrazioak detektatzeko, sistemak eta aplikazioak eguneratuta mantentzea eta EDR konponbideak erabiltzea portaera susmagarriak identifikatzeko. Gainera, oraindik ere funtsezkoa da langileak etengabe prestatzea phishing-detekzioari eta segurtasun-jardunbide egokiei buruz, infekzioak hasierako faseetatik prebenitzeko.

