ANDORRA DIGITAL

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

Informe d'Actor d'Amenaça

APT29

TLP: WHITE

29/09/2023

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	29-09-2023	29-09-2023

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi
2.0	29	29-09-2023	Traducció i maquetació

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGÍA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). Es tracta d'un esquema creat per fomentar un millor intercanvi d'informació de caràcter delicat (però no classificada) en l'àmbit de la seguretat de la informació. A través d'aquest esquema, d'una forma àgil i senzilla, s'indica fins a on pot circular la informació més enllà del receptor en qüestió, i aquest ha de consultar a l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra) [https://www.anc.ad/] quan la informació necessiti ser distribuïda a tercers.

CODI	QUAN EMPRAR-LO	COM COMPARTIR-LO
TLP:RED	S'ha d'utilitzar **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, reputació o operacions si és mal utilitzada.	Els receptors no han de compartir informació designada com **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP:AMBER	S'ha d'usar **TLP:AMBER** quan la informació requereix ser distribuïda de manera limitada, però suposa un risc per a la privacitat, reputació o operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com **TLP:AMBER** únicament amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per a protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per a compartir aquesta informació.
TLP:GREEN	S'ha d'emprar **TLP:GREEN** quan la informació és útil per a totes les organitzacions que participen, així com amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP:WHITE	S'ha d'utilitzar **TLP:WHITE** quan la informació no suposa cap risc de mal ús, dins de les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de Copyright.

2. INTRODUCCIÓ

Aquest informe constitueix un document estratègic que es centra en l'actor de l'amenaça conegut com APT29. L'objectiu fonamental d'aquest document consisteix a proporcionar una panoràmica completa i una comprensió precisa d'aquest actor d'amenaça. Amb aquest propòsit, s'hi exposaran les característiques rellevants, el modus operandi, les campanyes principals, les vulnerabilitats conegudes com a CVE (Common Vulnerabilities and Exposures) i els indicadors de compromís (IOCs).

Amb l'objectiu de facilitar la comprensió d'aquest actor d'amenaça, primerament, es brindarà una explicació sobre què és exactament una amenaça persistent avançada, anomenada comunament APT (Advanced Persistent Threat) en anglès. En aquest context, també es mostraran els actors d'amenaça APT, els quals es componen de grups finançats per l'estat i col·lectius de ciberdelinqüents. És notori el fet que aquests actors es destaquen per perseguir diferents objectius i emprar tàctiques diversificades.

APT29 ha cridat l'atenció a causa d'una extensa sèrie d'activitats malicioses que se li atribueixen i que han estat en curs, com a mínim, des de l'any 2008. S'insinua que aquest actor d'amenaça té connexions amb el Govern Rus i que mostra un elevat grau de sofisticació en les seves operacions de ciberatac. En conseqüència, planteja un risc significatiu per totes les organitzacions que poden ser objecte dels seus atacs.

És rellevant destacar que la identificació i el monitoratge constants dels actors d'amenaça són imperatius per la mitigació dels riscs associats a les activitats cibernètiques malicioses. Aquest informe es presenta com una eina essencial per tal de proporcionar informació als professionals de la seguretat i als responsables de la presa de decisions, amb l'objectiu de què puguin prendre les mesures pertinents per salvaguardar els seus actius digitals i defensar-se de les amenaces plantejades per aquest actor en particular.

3. AMENAÇA PERSISTENT AVANÇADA

Per posar en context i comprendre l'actor d'amenaça APT29 explicarem, en primer lloc, el concepte d'Amenaça Persistent Avançada (APT) i qui són els actors d'APT.

3.1. Què és un APT?

Analitzem els seus termes per separat:

- Amenaça: suposa un risc o un perill per la víctima.
- Persistent: s'estén amb el transcurs del temps.
- Avançada: empra tècniques complexes i sofisticades.

Una amenaça persistent avançada (APT) és un atac cibernètic prolongat i dirigit en què un intrús obté accés a una xarxa i roman sense ser detectat durant un període de temps. La intenció d'un atac APT generalment és monitoritzar l'activitat de la xarxa i robar dades, en lloc de causar danys a la xarxa o l'organització. El NIST (Institut Nacional d'Estàndards i Tecnologia) les defineix com amenaces "amb nivells sofisticats d'experiència i importants recursos que els permeten crear oportunitats per assolir els seus objectius utilitzant múltiples vectors d'atac".

Atès el gran esforç que es requereix per dur a terme un atac d'aquesta naturalesa, les APT solen tenir objectius de gran valor, com ara governs i grans corporacions, amb la finalitat de robar informació durant un període prolongat, a diferència dels ciberatacs de menor nivell on els ciberdelinqüents entren i surten ràpidament d'un sistema.

Les APT es consideren amenaces greus i costoses, per la qual cosa haurien d'estar en el focus d'atenció de les empreses arreu del món. A continuació, esmentem les seves característiques principals:

- Empren tècniques avançades i complexes pels atacs. Això inclou programari maliciós com botnets o exploits de zero-day, així com tècniques sofisticades d'enginyeria social.
- Són difícils de detectar ja que un dels objectius dels ciberdelinqüents és passar desapercebuts pels sistemes de seguretat de la víctima.
- Cerquen romandre als equips o sistemes de la víctima durant el màxim temps possible. Per fer-ho, s'adapten als esforços o tècniques de ciberseguretat que implanta la víctima i mantenen un alt nivell d'interacció i control dels seus equips.
- Es desenvolupen al llarg de diverses fases. Comencen per l'obtenció de l'accés i continuen amb la infecció dels equips, l'expansió del control i l'aprenentatge "des de dins" per descobrir noves vulnerabilitats.
- Requereixen elevats coneixements de tècniques de pirateig i una gran quantitat de recursos, pel que solen ser portades a terme per grups organitzats, els quals tenen molt d'interès en les víctimes dels seus ciberatacs.

- Les víctimes solen ser grans empreses i corporacions, governs o altres entitats responsables de la seguretat nacional.

Tot i que els atacs APT poden ser difícils d'identificar, el robatori de dades mai és completament indetectable. No obstant això, l'extracció de dades d'una organització pot ser l'única pista que tenen els defensors que les seves xarxes estan sota atac. Els professionals de la ciberseguretat sovint es centren a detectar anomalies en les dades sortints per veure si la xarxa ha estat l'objectiu d'un atac APT.

3.2. Què és un actor d'amenaça APT?

Un conjunt d'actors de amenaces altament sofisticats, coneguts com a APT (Amenaces Persistents Avançades), ha atret una atenció significativa a causa de les seves operacions altament complexes. Aquests grups d'APT inclouen pirates informàtics patrocinats per l'estat, organitzacions clandestines i col·lectius de ciberdelinqüents, i són amplament reconeguts pels seus diversos objectius i tàctiques.

Com s'ha esmentat, en ocasions aquests grups estan subvencionats o gestionats per governs i se centren en la manipulació de la informació de seguretat nacional. És comú que aquest tipus d'atacants se centrin en objectius d'importància geopolítica i que les seves accions tinguin un impacte substancial, no cessant fins que aconsegueixen els seus objectius.

Els motius que impulsen els actors d'amenaces avançades i persistents són diversos. Per exemple, els atacants patrocinats per estats nacionals poden buscar la propietat intel·lectual amb l'objectiu d'obtenir una avantatge competitiu en sectors industrials específics. Altres objectius poden abastar serveis de distribució d'energia i telecomunicacions, així com altres sistemes d'infraestructura crítica, xarxes socials, organitzacions de mitjans de comunicació i fins i tot objectius relacionats amb eleccions i altres afers polítics. A més, també és comú que grups de criminalitat organitzada portin a terme aquest tipus de ciberatacs amb l'ànim de dur a terme activitats delictives amb finalitats lucratives.

Els actors d'amenaces APT tendeixen a dirigir els seus esforços cap a organitzacions en sectors com la defensa nacional, la indústria manufacturera i el sector financer, ja que aquestes empreses gestionen informació de gran valor, que inclou propietat intel·lectual, plans militars i altres dades sensibles de governs i organitzacions empresarials.

A continuació, es presenta una taula on hi consten actors APT:

Actor de amenaza	Alias	País
APT28	Fancy Bear, Sofacy, PawnStorm, Sednit, Strontium	Rússia
APT29	Cozy Bear, The Dukes, CozyDuke	Rússia

APT30	APT-C-01	República Popular de la Xina
APT31	Zirconium, Judgment Panda, Stonesoft, Axiom, Bronze Panda	República Popular de la Xina
APT32	OceanLotus, SeaLotus, Cobalt Kitty, APT-C-00, OceanBuffalo	Vietnam
APT33	Elfin, Refined Kitten, Holmium, Magnallium	República Islàmica de l'Iran
APT34	OilRig, Helix Kitten, Chrysene	República Islàmica de l'Iran
APT35	Newscaster, Charming Kitten, Phosphorus, Ajax Security Team	República Islàmica de l'Iran
APT36	Transparent Tribe, ProjectM, Mythic Leopard, TEMP.La	República Islàmica del Pakistan
APT37	Reaper, StarCruft, Group123, Ricochet Chollima, RedEyes	República Popular Democràtica de Corea
APT38	Lazarus Group, Hidden Cobra, Guardians of Peace	República Popular Democràtica de Corea
APT39	Chafer, Remexi, Cadelspy	República Islàmica de l'Iran
APT40	Periscope, Mudcarp, TEMP.Periscope, TEMP.Jumper, Leviathan	República Popular de la Xina
APT41	Double Dragon, Winnti, Barium, Wicked Panda, Wicked Spider	República Popular de la Xina

Amb l'objectiu d'aconseguir l'accés als sistemes de les seves víctimes, els grups d'APT sovint recorren a mètodes d'atac avançats, que inclouen l'ús d'exploits sofisticats per a vulnerabilitats de zero-DAY, així com l'*spear phishing* (una modalitat de *phishing* dirigida específicament a un objectiu) i altres tècniques d'enginyeria social. Per a mantenir l'accés a la xarxa objectiu sense ser detectats, els actors d'amenaces utilitzen mètodes avançats, com ara la constant reescriptura del codi maliciós per evitar la detecció i altres tècniques sofisticades d'evasió. Algunes APT són tan complexes que requereixen administradors a temps complet per mantenir els sistemes i el programari compromès dins de la xarxa objectiu.

4. PERFIL DE L'ACTOR D'AMENAÇA APT29

Després d'haver explicat el concepte d'amenaça persistent avançada (APT) i qui en són els actors d'amenaça d'APT, ens centrarem en l'actor d'amenaça APT29. Explicarem qui és aquest actor, quins són els seus objectius i motivacions, així com el seu modus operandi.

4.1. Qui és APT29?

APT29 és un actor d'amenaça persistent avançada (APT) actiu des del 2008 i opera en el context del Servei d'Intel·ligència Exterior de la Federació Russa (SVR RF), una agència d'intel·ligència que té capacitats transgressores per dur a terme operacions avançades de ciber-espionatge.

APT29 té una gran disciplina tècnica i sofisticació, especialment en la seva capacitat per a adaptar-se a tàctiques defensives de seguretat de TI, penetrar xarxes ben defensades i implementar programari maliciós amb capacitats anti-forenses.

Alies

APT29 també és conegut per altres noms como AKA CozyBear, The Dukes, Group 100, CozyDuke, EuroAPT, CozyCar, Cozer, Office Monkey, YTTRIUM, Iron Hemlock, Iron Ritual, Cloaked Ursa, Nobelium, Group G0016, UNC2452, Dark Halo, NobleBarron, SolarStorm, StellarParticle.

Objectiu

APT29 té com a objectiu principal pertorbar la seguretat nacional, impactar la infraestructura crítica i causar interferència política.

Sectors objectiu

Els sectors objectiu són els governs i subcontractistes governamentals, organitzacions polítiques, empreses de recerca i indústries crítiques com l'energia, l'atenció mèdica, l'educació, les finances i la tecnologia.

També s'ha identificat com a objectiu a organitzacions associades amb l'extremisme txetxè; els parlants de rus que participen en el comerç il·lícit de substàncies i drogues controlades; i objectius diplomàtics, de *think tanks*, sanitaris i energètics.

Països objectiu

Els Estats Units, països d'Europa i membres de l'OTAN. Entre ells destaquen els governs dels membres de la Commonwealth; també països d'Àsia, Àfrica i Mitjà Orient.

Motivacions

Com s'ha esmentat, les activitats del grup tenen els seus orígens en motivacions polítiques i geopolítiques, centrant-se en la recopilació d'intel·ligència i l'àmbit de l'espionatge cibernètic.

Les motivacions d'APT29 es poden inferir després d'observar les estratègies que apliquen dins del context de les seves campanyes. El grup és conegut pel seu interès en dades geopolítiques secretes que serien avantatjoses pel govern rus.

4.2.Campanyes rellevants

APT ha estat responsable de diverses campanyes notables, inclòs l'atac a la cadena de subministrament de SolarWinds. A continuació, comentem algunes de les seves campanyes més rellevants:

2008: Txetxènia

La primera activitat que s'ha pogut atribuir definitivament a APT29 són dues campanyes del programari maliciós «PinchDuke» al novembre de 2008. Aquestes campanyes utilitzaven mostres de PinchDuke que, segons registres, van ser creades els dies 5 i 12 de novembre de 2008. Els investigadors de la campanya van trobar dues mostres, les quals són “alkavkaz.com20081105” i “cihaderi.net20081112”.

2014: Instituts d’Investigació i agències dels Estats Units

Les campanyes de correu electrònic no desitjat del 2014 tenien com a objectiu plantar el programari maliciós «CozyDuke» i «Miniduke» en instituts de recerca i agències estatals als Estats Units.

2015: Pentàgon

Aquest ciberatac d'*spear phishing* va paralitzar el sistema de correu electrònic del Pentàgon per un temps. APT29 va obtenir accés inicial a la xarxa del Pentàgon mitjançant phishing i va introduir la tècnica "Hammertoss" per a utilitzar comptes ficticis de Twitter per a la comunicació C2.

2015: Grizzly Sttepe

En aquesta campanya coneguda com a "Grizzly Steppe", APT29 va violar els servidors del Comitè Nacional Demòcrata prop de les eleccions estatunidenques a través d'una campanya de *phishing* que demanava a les víctimes que canviessin les seves contrasenyes utilitzant un lloc web fals.
La campanya de *phishing* executada per APT29 va ser dirigida a més 1.000 adreces de correu electrònic als quals es va enviar contingut maliciós a través d'un enllaç, incloses nombroses víctimes governamentals. Almenys un dels receptors, va activar els enllaços que contenien programari maliciós. En aquesta campanya, APT29 va comprometre reeixidament a un partit polític dels Estats Units.

Així mateix, es va realitzar una sèrie d'atacs contra ONG i *think tanks* amb seu als Estats Units.

2017: Govern de Noruega

L'atac de phishing dirigit al govern noruec el gener del 2017 va afectar al Partit Laborista del país, al Ministeri de Defensa i al Ministeri de Relacions Exteriors.

2019: Ministeris de la UE i ambaixada de la UE

APT29 va comprometre tres ministeris d'Assumptes Nacionals de la Unió Europea i a una ambaixada de la mateixa amb seu a Washington D.C. als Estats Units.

Aquest atac correspon a una onada d'infeccions cibernètiques de tipus «Operation Ghost» del 2019, la qual va introduir les noves famílies de programari maliciós Polyglot Duke, RegDuke i FatDuke.

2020: Dades de la vacuna per la COVID-19

El juliol de 2020, centres de ciberseguretat de tot el món van acusar APT29 de perpetrar un furt d'informació i propietat intel·lectual relacionades amb el desenvolupament de les vacunes i les proves de la COVID-19, al Canadà, el Regne Unit i els Estats Units. Els investigadors van indicar que el grup va utilitzar programari maliciós personalitzat com WellMess i WellMail per tal de realitzar els atacs.

2020: FireEye

El desembre del 2020, un grup patrocinat per l'Estat rus va atacar FireEye, una empresa de ciberseguretat estatunidenca. Els atacants varen piratejar la xarxa de FireEye i van robar eines que després van usar per a testar la defensa dels clients de FireEye, inclosos els governs federal,

estatal i local dels Estats Units, així com a governs locals i grans corporacions globals. Encara que no s'ha confirmat la identitat dels atacants, el principal sospitós de l'incident, segons els investigadors, era APT29.

2021: Organitzacions amb seu als Estats Units i Europa

El maig del 2021, un grup d'investigadors va identificar una campanya de phishing dirigida a organitzacions amb seu als Estats Units i Europa. Els correus electrònics de phishing provenien suposadament de l'Agència dels Estats Units per al Desenvolupament Internacional (USAID, per les seves sigles en anglès) i contenia diversos arxius maliciosos i un cimbell legítim. Encara que la identitat dels atacants no ha pogut ser confirmada, els investigadors creuen que l'actor d'amenaça darrere de la campanya és APT29.

2021: Comitè Nacional Republicà

El juliol de 2021, APT29 va atacar a Synnex, un contractista que brinda serveis de TI pel Comitè Nacional Republicà (RNC), un comitè polític dels Estats Units. El Comitè Nacional Republicà va declarar que es va bloquejar tot l'accés des dels comptes de Synnex al seu entorn cloud després del ciberatac, i que no es va accedir a cap dada del RNC.

2023: Diplomàtics de Kiev

Els ciberdelinqüents van utilitzar un volant legítim de la missió polonesa per intentar infiltrar un programari maliciós entre diplomàtics estrangers a Kíev al llarg del 2023. Un diplomàtic del Ministeri d'Afers exteriors polonès va enviar per correu electrònic un volant legítim a diverses ambaixades anunciant la venda d'un vehicle sedan de la marca BMW, concretament un sèrie 5 de segona mà i que es podia trobar a la ciutat de Kíev, Ucraïna. El diplomàtic polonès, que no va voler ser identificat per motius de seguretat, va confirmar el paper del seu anunci en la intrusió digital. Els pirates informàtics van interceptar i van copiar aquest document, li van afegir programari maliciós i després el van enviar a dotzenes d'altres diplomàtics estrangers que treballen a Kíev.


CAR FOR SALE IN KYIV
THE PRICE IS REDUCED!!!
BMW 5 (F10) 2.0 TDI, 7,500 Euros!!
Very good condition, low fuel consumption
More high quality photos are here: https://t.ly/

Model	BMW 5, 2.0 TDI (184 HP)
Year	April 2011
Mileage	266,000 km
Engine	2.0 Diesel
Transmission	Mechanic
Colour	Black, black leather interior
Package	A/C, set of summer and winter tires, ABS/ESP, led lights, cruise control, multifunction steering wheel, CD, electric seats, electric windows, engine control, rain sensor, electrical hand brake, airbags, start-stop system.
Price	7,500 Euros
Custom	NOT CLEARED
Contact	

Figure 1. Example lure used in BMW campaign.
(SHA256: 311e9c8cf6d0b295074ffefaa9f277cb1f806343be262c59f88fbdf6fe242517)

Imatge 1: Anunci fals d'automòbils de segona mà creat per ciberdelinqüents en un intent d'accedir als ordinadors de desenes de diplomàtics en ambaixades d'Ucraïna (Font: REUTERS/Unit42)

2023: Ministeris d'Assumptes Exteriors de diversos països de l'OTAN

La recent campanya del 2023 realitzada per APT29 va recórrer a l'ús de correus brossa en atacs dirigits. Aquests, van ser enviats als ministeris d'Afers Exteriors que eren d'interès per la Federació Russa, és a dir, organismes alineats amb l'OTAN. Els correus contenien arxius PDF maliciosos que es camuflaven com a invitacions diplomàtiques procedents d'una ambaixada alemanya.

En una de les operacions de correu brossa, no es va incorporar una càrrega útil. El document titulat "Dia de la Unió Alemanya" enviava una notificació als atacants quan s'obria l'arxiu adjunt al correu electrònic. Això insinua que podria haver estat una operació de reconeixement o una prova per avaluar les taxes d'èxit de l'estratagema.

En la segona campanya, es va distribuir un arxiu PDF amb el nom "*Farewell to Ambassador of Germany*" (Comiat de l'ambaixador d'Alemanya) que contenia una variant del programari maliciós Duke. Aquest document incloïa codi JavaScript incrustat, el qual es va utilitzar per lliurar una càrrega útil en múltiples fases en format HTML.

Si l'usuari obria el PDF amb Adobe Acrobat (o una aplicació similar), se li plantejava una consulta sobre el codi incrustat i la seva execució. En cas que la víctima ho autoritzés, es desencadenava un document HTML maliciós titulat "Invitation_Farewell_DE_EMB"

A continuació, la cadena avançava fins a l'obtenció d'un arxiu ZIP que contenia una aplicació HTML (HTA). La cadena va passar per diverses fases addicionals fins que el programari maliciós Duke va aconseguir infiltrar-se amb èxit.

Imatge 2: Adjunt maliciós que distribueix la variant de programari maliciós «Duke».

4.3. Eines utilitzades

Al llarg dels anys, APT29 ha implementat una àmplia varietat d'eines. És important subratllar que la possibilitat que aquest actor introdueixi nous conjunts d'eines de programari maliciós continua sent considerable, tret que les seves operacions es detinguin. La naturalesa de les seves activitats suggereix un potencial sostingut d'innovació en les seves estratègies i tècniques.

El següent és un llistat cronològic d'alguns dels conjunts d'eines més coneguts utilitzats per aquest grup.

PinchDuke

Es considera que aquest va ser el primer conjunt d'eines àmpliament atribuït a APT29. El kit d'eines consisteix en múltiples *loaders* (un *loader* és un codi maliciós que s'inicia després que un usuari inicia el programa *dropper*, sigui en obrir o en executar un arxiu) i un troià lladre d'informació. El programari maliciós recopila informació de configuració del sistema, roba credencials d'usuari i recopila arxius d'usuari del host compromès, transferint-los a través d'HTTP(S) a un servidor C2.

Es va reportar que PinchDuke ha estat utilitzat des de novembre del 2008 fins a l'estiu de 2010 i es va observar en atacs contra Txetxènia, Turquia, Geòrgia, i diversos antics estats soviètics, abans d'evolucionar al conjunt d'eines CosmicDuke en 2010.

GeminiDuke

Té capacitats de *loader* i múltiples mecanismes d'assegurament de la persistència. Així mateix, compta amb funcionalitats de *stealer* (lladre d'informació) utilitzades predominantment per a la recopilació de dades de configuració de dispositius.

La informació d'interès d'APT29 inclou: comptes d'usuari, controladors i programari instal·lat, processos en execució, programes/serveis iniciats en arrencar, configuracions de xarxa, carpetes/arxius presents en ubicacions específiques, programes executats recentment i carpetes/arxius oberts, etc.

GeminiDuke es va usar activament des de gener de 2009 fins a desembre de 2012.

CosmicDuke

També conegut com BotgenStudios, NemesisGemina, Tinybaron, aquest gira principalment entorn a les seves capacitats de furt d'informació. Pot filtrar arxius amb extensions específiques, exportar certificats criptogràfics (incloses claus privades), realitzar capturar captures de pantalla, registrar pulsacions de tecles (keylogging), extreure credencials d'inici de sessió (navegadors, clients de correu electrònic i missatgers), així com recopilar contingut del porta-retalls (búfer copiar-pegar).

CosmicDuke es va utilitzar des de gener de 2010 fins a l'estiu de 2015 i es va observar que tenia com a objectiu una àmplia gamma d'organitzacions, incloses aquelles dels sectors d'energia i telecomunicacions, i governs i militars.

MiniDuke

És un programari maliciós que ve en diverses iteracions que abasten funcionalitats de *loader*, *downloader* (amenaça informàtica l'única funcionalitat de la qual és descarregar el programari maliciós principal en l'equip compromès) i *backdoor* (entrada secreta que s'empra com a control remot per a fins maliciosos). MiniDuke s'utilitza, principalment, per a preparar un sistema per a infeccions posteriors i/o facilitar la progressió d'aquestes infeccions.

CozyDuke

També conegut com a Cozer, CozyBear, CozyCar, EuroAPT. Aquest, funciona, principalment, com un *backdoor*. El seu objectiu principal és establir un punt d'entrada per a infeccions posteriors, en particular els seus propis mòduls. Per a això, empra un *dropper* (virus troià que conté un arxiu executable) i múltiples mòduls per a garantir la persistència.

Entre els seus components, es troben aquells que s'encarreguen d'extreure dades del sistema, executar comandos bàsics de Cmd.exe, realitzar captures de pantalla i robar credencials d'inici de sessió. No obstant això, CozyDuke posseeix la capacitat d'infiltrar-se i executar altres arxius, la qual cosa evidencia el seu potencial per a facilitar qualsevol tipus d'infecció de programari maliciós.

APT29 va utilitzar CozyDuke des de gener de 2010 fins a la primavera de 2015.

OnionDuke

És un programari maliciós modular amb una varietat de configuracions potencials. Té capacitats de *loader* i *dropper.* El programa implementa diversos mòduls diferents de robatori d'informació, per exemple, per a recopilar contrasenyes i altres dades confidencials. També té un component per a llançar atacs DDoS (Denegació de Servei Distribuïda). Un altre mòdul està dissenyat per a utilitzar comptes de xarxes socials compromeses per a llançar campanyes de contingut brossa, la qual cosa podria propagar l'abast de la infecció.

Es va observar l'ús d'OnionDuke des de febrer de 2013 fins a la primavera de 2015.

SeaDuke

També conegut com a SeaDaddy, SeaDask, és un *backdoor* multiplataforma dissenyat per operar en sistemes Windows i Linux. Malgrat la seva relativa simplicitat, serveix com un conjunt d'eines l'objectiu principal de les quals és executar els arxius infiltrats, propagant així la infecció.

SeaDuke va estar actiu des d'octubre de 2014 fins a maig de 2016 i va ser observat durant l'atac del DNC per APT29 en 2015.

HammerDuke

També conegut com a HAMMERTOSS, Netduke, és un backdoor, l'ús del qual, ha estat exclusivament com backdoor secundari que segueix a una infecció de CozyDuke.
HammerDuke va ser utilitzat des d'almenys gener de 2015 fins a juliol de 2015.

CloudDuke

També conegut com a CloudLook, MiniDionis. Es manifesta en dues versions de *backdoor*. Aquest programari maliciós també inclou funcions de *downloader* (descàrrega) i *loader* (càrrega). Aquestes funcions són dirigides, principalment, a obtenir i instal·lar càrregues útils des d'ubicacions predeterminades, sigui des d'Internet o des d'un compte de Microsoft OneDrive.

CloudDuke es va usar, principalment, durant l'estiu de 2015.

Cobalt Strike Beacon

En la campanya de *phishing* de novembre de 2018 vinculada a APT29, aquest va utilitzar Cobalt Strike Beacon en lloc de qualsevol programari maliciós o kit d'eines personalitzat. La càrrega útil de Beacon es va configurar amb una variació modificada del perfil de C2 "Pandora" Maleable disponible públicament i va fer servir el domini C2: pandorasong[.]com.

PowerDuke

PowerDuke ha estat propagat a les víctimes via correu electrònic amb arxius Microsoft Word o Excel amb macros maliciosos. Si s'explota amb èxit, es descarrega una imatge PNG del servidor web compromès i s'oculta el troià PowerDuke ocult en les imatges PNG mitjançant esteganografia.

PowerDuke es va veure per primera vegada l'agost de 2016 i es va utilitzar en la campanya de phishing postelectoral de novembre de 2016.

Poshpy

És un backdoor que aprofita PowerShell i Windows Management Instrumentation (WMI). El seu ús d'una càrrega útil de PowerShell significa que només s'utilitzen processos legítims del sistema i que l'execució de codi maliciós només pot identificar-se a través d'un registre millorat o en la memòria.

Poshpy ha estat actiu almenys des d'inicis de 2015.

4.4. Vulnerabilitats explotades

En el següent llistat podem veure les vulnerabilitats explotades per APT29:

CVE-ID	Severitat	Descripció	Tipus d'explotació
CVE-2018-13379 (Fortinet FortiOS)	CVSSv3 Puntuació: 9.8 – Crítica	Una limitació inapropiada d'un Pathname a un Directori restringit ("Path Traversal") en SSL VPN Portal, permet a un actor d'amenaça no autenticat la descàrrega d'arxius a través de sol·licituds de recursos HTTP especialment manipulats.	WebApp
CVE-2019-9670 (Zimbra Collaboration Suite)	CVSSv3 Puntuació: 10.0 – Crítica	La vulnerabilitat d'injecció d'entitat externa (XML, també coneguda com XXE) al component de bústia de correu de Synacor Zimbra Collaboration Suite.	Execució de codi remota
CVE-2019-11510	CVSSv3 Puntuació: 10.0 – Crítica	L'explotació exitosa d'aquesta vulnerabilitat permet a un actor d'amenaça remota no autenticat enviar un URI (Uniform Resource Identifier) especialment dissenyat per a realitzar una vulnerabilitat de lectura d'arxius arbitrària.	WebApp
CVE-2019-19781 (Citrix ADC Network Gateway)	CVSSv3 Puntuació: 9.8 – Crítica	S'ha descobert un problema a Citrix Application Delivery Controller (ADC) que permet un salt de directoris (Directory Traversal).	Execució de codi remota
CVE-2020-4006 (VMware Workspace ONE Access)	CVSSv3 Puntuació: 9.1 – Crítica	Vulnerabilitat d'injecció d'ordres.	

4.5. Indicadors de Compromís (IOC)

Direccions IP associades:

- 193[.]36[.]119[.]162
- 91[.]132[.]139[.]195
- 141[.]255[.]164[.]11
- 193[.]36[.]116[.]119
- 185[.]99[.]133[.]226
- 5[.]252[.]177[.]21
- 111[.]90[.]150[.]140
- 23[.]106[.]123[.]15
- 111[.]90[.]147[.]248
- 141[.]255[.]164[.]40
- 91[.]234[.]254[.]144
- 31[.]42[.]177[.]78
- 141[.]255[.]164[.]36
- 193[.]239[.]84[.]199
- 193[.]36[.]119[.]184
- 185[.]66[.]91[.]180
- 107[.]152[.]35[.]77
- 111[.]90[.]151[.]120
- 13[.]57[.]184[.]217
- 13[.]59[.]205[.]66

Dominis associats:

- avsvmcloud[.]com
- literaturaelsalvador[.]com
- signitivelogics[.]com
- totalmassasje[.]no
- 2bdo5s70oc51vu3de3bvrq60eiw[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
- 2e7hv525mpn9uiljt3ev[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
- 7sbvaemscs0mc925tb99[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
- 8cngei63kcpgho7kern0le2ve2sn0te2[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
- 8tvp0990935eitt5hjvcbmv[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
- act4fk13agv8olsou30e2st[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
- appsync-api[.]us-east-1[.]avsvmcloud[.]com
- athe4f602s6ce101uj21[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
- gq1h856599gqh538acqn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
- hvpgv9psvq02ffo77et[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
- ihvpgv9psvq02ffo77et[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
- jbq3rh7rjdghmmcxco0ge2sd[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
- k5kcubuassl3alrf7gm3[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
- ld3iu5dr2341o83hhr5p[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
- mhdosoksaccf9sni9icp[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com

Hashes (SHA256) d'arxius associats:

- 019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
- 0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
- 1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
- 1cffaf3be725d1514c87c328ca578d5df1a86ea3b488e9586f9db89d992da5c4
- 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
- 381a3c6c7e119f58dfde6f03a9890353a20badfa1bfa7c38ede62c6b0692103c

Hashes (SHA1) d'arxius associats:

- 1acf3108bf1e376c8848fbb25dc87424f2c2a39c
- 1fb12e923bdb71a1f34e98576b780ab2840ba22e
- 2f1a5a7411d015d01aaee4535835400191645023
- 395da6d4f3c890295f7584132ea73d759bd9d094
- 72e5fc82b932c5395d06fd2a655a280cf10ac9aa
- 75af292f34789a1c782ea36c7127bf6106f595e8
- 76640508b1e7759e548771a5359eaed353bf1eec
- 9858d5cb2a6614be3c48e33911bf9f7978b441bf

Hashes (MD5) d'arxius associats:

- 1c3b8ae594cb4ce24c2680b47cebf808
- 2c4a910a1299cdae2a4e55988a2f102e
- 56ceb6d0011d87b6e4d7023d7ef85676
- 731d724e8859ef063c03a8b1ab7f81ec
- 846e27a652a5e1bfbd0ddd38a16dc865
- 9466c865f7498a35e4e1a8f48ef1dffd

4.6. Tècniques utilitzades

El grup APT29 existeix des de fa més d'una dècada i ha utilitzat diverses tècniques sofisticades per a proliferar els seus programes maliciosos, a través de programari maliciós personalitzat. En general, aconsegueix els seus objectius a través d'arxius binaris compilats personalitzats i mètodes d'execució alternatius, com PowerShell i

Windows Management Instrumentation (WMI). També se sap que APT29 empra diverses cadències operatives (aixafar i agarrar versus lent i deliberat) depenent del valor d'intel·ligència percebut i/o del mètode d'infecció de les víctimes.

Encara que, com hem esmentat, les tècniques usades canvien amb el temps presentem un panorama d'aquelles que ha vingut utilitzant en les diferents etapes dels ciberatacs duts a terme.

Accés inicial

APT29 ha utilitzat el spear phishing com a vector d'atac inicial. Inicialment, això implicava principalment l'ús d'un arxiu adjunt per a lliurar arxius amb exploits a les víctimes inicials. Des de 2015, això ha evolucionat al spear phishing que busca enganyar les víctimes perquè facin clic en un enllaç per a descarregar un document cimbell legítim juntament amb un arxiu d'accés directe de Windows maliciós (LNK), mentre que a vegades usa dominis legítims compromesos. Això es va observar en la campanya de phishing de 2018 i en la campanya PowerDuke de 2016.

Execució

APT29 utilitza principalment tàctiques de seqüències d'ordres, PowerShell, execució de serveis, WMI i explotació per a execució de clients per a aconseguir l'execució en entorns específics. Des de 2014, els atacs i les eines desenvolupades per APT29 solen usar scripts de PowerShell per a descarregar/instal·lar i executar comandos, així com per a evadir la detecció.

Persistència

APT29 ha utilitzat habitualment tàctiques de tasques programades, claus d'execució del registre i subscripció a esdeveniments WMI per a mantenir la persistència en les xarxes objectiu. En particular, les seves tècniques han progressat fins a utilitzar WMI Event Subscription per a mantenir la persistència a través de la seva backdoor Poshspy des d'aproximadament 2015.

Escalada de privilegis

Es té informació que APT29 ha explotat vulnerabilitats, eludint el Windows User Account Control (UAC) i utilitzant funcions d'accessibilitat per a escalar privilegis. Més notablement, això va implicar l'ús de la funció d'accessibilitat "Sticky Keys" des d'aproximadament 2014 d'ara

endavant. Usant un script de PowerShell per a instal·lar un servei de Tor, van poder substituir el codi binari de Sticky Keys pel processador d'ordres de Windows "cmd.exe".

Evasió de defensa

La majoria de les tècniques d'evasió de defensa utilitzades per APT29 s'han implementat a partir de l'any 2014. Entre elles es troben l'ofuscament d'arxius o informació, l'eliminació d'arxius, l'eliminació d'indicadors al host i la utilització de scripts PowerShell per descarregar i/o instal·lar o executar ordres.

Accés de credencials

Les primeres famílies de programari maliciós d'APT29 utilitzaven el bolcat de credencials i la captura/keylogging d'entrada. El grup també ha estat vinculat a eines comercials amb capacitat d'accés a credencials, com Mimikatz i Cobalt Strike.

Descobriment

PowerDuke, atribuït a APT29 al llarg del 2016, conté diverses ordres per obtenir informació del sistema. Per exemple, PowerDuke té ordres per aconseguir text de la finestra actual en primer pla, per accedir al seu nom de directori actual, així com la grandària d'un arxiu, pel nom i el SID de l'usuari actual i també per informació sobre la víctima.

Moviment lateral

APT29 ha utilitzat tradicionalment tècniques de còpia remota d'arxius, *pass the hash*, *pass the ticket* y Windows Admin Shares per moure's lateralment en entorns objectiu. En particular, amb algunes variants del programari maliciós SeaDuke a partir d'octubre de 2014, APT29 va usar un atac Kerberos golden tiquet a través de Mimikatz.

Recopilació

APT29 ha utilitzat diverses tècniques de recopilació, inclosa la captura de dades del sistema local, mitjans extraïbles, unitats compartides en xarxa, el porta-retalls i Microsoft Outlook.

Exfiltració

APT29 ha utilitzat comptes vàlids, exfiltració a través de protocols alternatius, exfiltració automatitzada i compressió de data per exfiltrar dades. Per exemple, s'ha vist a Hammertoss pujar informació de les xarxes de les víctimes a comptes de serveis d'emmagatzematge al núvol, usant credencials d'inici de sessió rebudes mitjançant esteganografia.

Ordre i control

APT29 utilitza una sèrie de tècniques C2, que inclouen les següents:
- Protocol estàndard de capa d'aplicació.
- Protocol Criptogràfic Personalitzat.
- Protocol Criptogràfic Estàndard.
- Codificació de dades.
- Servei Web.
- Domini Fronting.

5. RECOMANACIONS

Davant l'amenaça del grup APT29 tant per empreses com organitzacions vinculades als governs, s'han d'establir mesures de protecció per evitar atacs per part d'aquest actor. A continuació, esmentem algunes mesures concretes que poden dur-se a terme:

- Atès que APT29 explota regularment vulnerabilitats conegudes públicament i duu a terme atacs complexos a la cadena de subministrament per obtenir accés inicial a les xarxes objectiu, és molt important gestionar i aplicar les actualitzacions de seguretat al més aviat possible amb la finalitat de reduir la superfície d'atac disponible.
- Han d'aplicar-se controls de seguretat de xarxa i gestió eficaç dels privilegis dels usuaris per a impedir el moviment lateral entre hosts, la qual cosa limitarà l'eficàcia dels atacs complexos.
- Les organitzacions han d'assegurar-se que s'habiliten *logs* (registres) als sistemes (tant en el núvol com *on-premise*) i que s'emmagatzemen durant un període de temps adequat, a fi d'identificar els comptes compromesos, el material filtrat i la infraestructura dels actors d'amenaces. És necessari habilitar aquests registres per conèixer l'activitat dels usuaris, que solen ser la baula més feble de la seguretat en una organització.
- També han d'aplicar-se polítiques de retenció de correu electrònic i de contingut per a reduir la quantitat d'informació delicada disponible en cas d'atac. Una política de retenció de dades ha de ser part de l'estratègia general de gestió de dades d'una organització. En el cas de la bústia de correu electrònic, la política de retenció estableix esborrar els missatges de correu electrònic de les bústies de correu dels usuaris després del període de temps que l'organització triï.
- Protegir els dispositius i les xarxes mantenint-los sempre actualitzats. Utilitzar les últimes versions compatibles, aplicar els pegats de seguretat sense demora, utilitzar plataformes antivirus i escanejar amb regularitat per a protegir-se de les amenaces de programari maliciós conegudes.
- Aplicar l'autenticació de doble factor per reduir l'impacte de les contrasenyes compromeses.
- Formar als usuaris perquè aquests siguin capaços d'actuar i informar sobre correus electrònics sospitosos de *phishing*.

6. GLOSSARI

APT (Advanced Persistent Threat)

Una amenaça avançada persistent (APT) utilitza tècniques d'atac continu, clandestí i avançat per accedir a un sistema i romandre-hi durant un temps prolongat, amb conseqüències potencialment destructives.

Backdoor

Una backdoor, com el seu nom indica, és una "entrada secreta" ja inclosa en el sistema en la majoria dels casos, que s'empra com a control remot per finalitats malicioses com, per exemple, infectar una varietat d'equips per formar una botnet.

Botnet

Una botnet o xarxa zombi és un grup d'ordinadors o dispositius que estan sota el control d'un atacant i que s'usen per perpetrar activitats malintencionades contra una víctima. El terme botnet és una combinació de les paraules robot i xarxa per representar la naturalesa d'un ciberatac realitzat mitjançant una botnet.

Ciberatac

Intent deliberat d'un ciberdelinqüent d'obtenir accés a un sistema informàtic sense autorització servint-se de diferents tècniques i vulnerabilitats per la realització d'activitats amb finalitats malicioses, com ara el robatori d'informació, l'extorsió del propietari o simplement danys al sistema.

CVE (Common Vulnerabilities and Exposures)

És una llista de vulnerabilitats i exposicions de seguretat de la informació divulgades públicament. CVE va ser llançat el 1999 per la corporació MITRE per identificar i categoritzar vulnerabilitats en programari i microprogramari. CVE proporciona un diccionari gratuït perquè les organitzacions millorin la seva seguretat cibernètica. MITRE és una organització sense ànim de lucre que opera centres de recerca i desenvolupament finançats amb fons federals als Estats Units.

DDoS (Denegació de Servei Distribuït)

Un atac DDoS, o atac distribuït de denegació de servei, és un tipus de ciberatac que intenta fer que un lloc web o recurs de xarxa no estigui disponible col·lapsant-lo amb trànsit maliciós perquè no pugui funcionar correctament.

Downloader

Amenaça informàtica l'única funcionalitat de la qual és descarregar el programari maliciós principal a l'equip compromès.

Dropper

És un tipus de programari maliciós que es caracteritza per contenir un arxiu executable, com pot ser un .exe, .msi, .docm, etc. Sovint, només està compost per un codi inofensiu a simple vista que s'activarà quan rebi l'ordre de descarregar el malware que s'encarregarà d'infectar la màquina.

Esteganografia

És la pràctica d'amagar informació dins d'un altre missatge o objecte físic per evitar-ne la detecció. Es pot utilitzar per amagar gairebé qualsevol mena de contingut digital, sigui text, imatges, vídeos o àudios. Després, aquestes dades ocultes s'extreuen en destí.

Exploit

Un exploit és un programa informàtic, una part d'un programari o una seqüència d'ordres que aprofita un error o vulnerabilitat per provocar un comportament no intencionat o inesperat en un programari, maquinari o en qualsevol dispositiu electrònic. Aquests comportaments inclouen, per regla general, l'agafada del control d'un sistema, la concessió de privilegis d'administrador a l'intrús o el llançament d'un atac de denegació de servei (DoS o DDoS).

Exploit de zero-day

Un exploit de zero-day és un error de seguretat no descobert prèviament en el vostre programari o maquinari i el qual els ciberdelinqüents poden aprofitar per penetrar en els vostres sistemes.

Enginyeria social

És un conjunt de tècniques que utilitzen els cibercriminals per enganyar els usuaris incauts perquè els enviïn dades confidencials, infectin les seves computadores amb programari maliciós o obren enllaços a llocs infectats.

IOC (Indications of Compromise)

Un Indicador de Compromís o IOC és un terme forense que es refereix a l'evidència en un dispositiu que assenyala una violació de seguretat. Les dades dels IOC es recopilen després d'un incident sospitós, un esdeveniment de seguretat o esdeveniments estranys a la xarxa.

Loader

Un loader (carregador) és un codi maliciós que s'inicia després que un usuari posa en marxa el programa dropper, sigui en obrir o en executar un arxiu.

Log

Els registres o logs fan referència als arxius de text en què s'inclouen de forma cronològica els esdeveniments com canvis, actualitzacions i altres que han ocorregut dins d'un sistema informàtic, com pot ser un servidor, una aplicació o un programa, així com la sèrie de modificacions que aquests han generat.

Logging

És una tècnica que consisteix en emmagatzemar una sèrie de successos que ocorren en una aplicació o sistema informàtic en un fitxer anomenat log.

Malware

És un tipus de programari que té com a objectiu danyar o infiltrar-se sense el consentiment del seu propietari en un sistema d'informació. Paraula que neix de la unió dels termes en anglès de programari maliciós: malicious software. Dins d'aquesta definició té cabuda un ampli ventall de programes maliciosos: virus, cucs, troyans, *backdoors*, *spyware*, etc. La nota comuna a tots aquests programes és el seu caràcter perniciós o perjudicial.

Path Traversal

El *path traversal*, *directory traversal* o, en català, salt de directoris és una tècnica de pirateig web que permet accedir a fitxers de l'aplicació per als quals no es hauria de tenir autorització. Aquest

ciberatac és possible quan les aplicacions presenten certes vulnerabilitats, que consisteixen a construir la ruta de descàrrega d'un fitxer mitjançant una entrada ingressada per l'usuari. Aquesta falta de validació de l'entrada pot ser explotada per un atacant per descarregar informació delicada, com dades personals i contrasenyes.

Phishing

És una tècnica d'enginyeria social que consisteix en l'enviament de correus electrònics que suplanten la identitat de companyies o organismes públics i sol·liciten informació personal i bancària a l'usuari. Mitjançant un enllaç inclòs en el correu electrònic, intenten redirigir-lo a una pàgina web fraudulenta perquè introdueixi el seu número de targeta de crèdit, DNI, la contrasenya d'accés a la banca en línia, etc.

Spear phishing

És una modalitat de *phishing* dirigida a un objectiu específic, en què els atacants intenten, mitjançant un correu electrònic, aconseguir informació confidencial de la víctima. Encara que el seu objectiu sovint és robar dades per a finalitats malicioses, els cibercriminals també poden intentar instal·lar programari maliciós a l'ordinador de la víctima.

CLÀUSULA DE CONFIDENCIALITAT