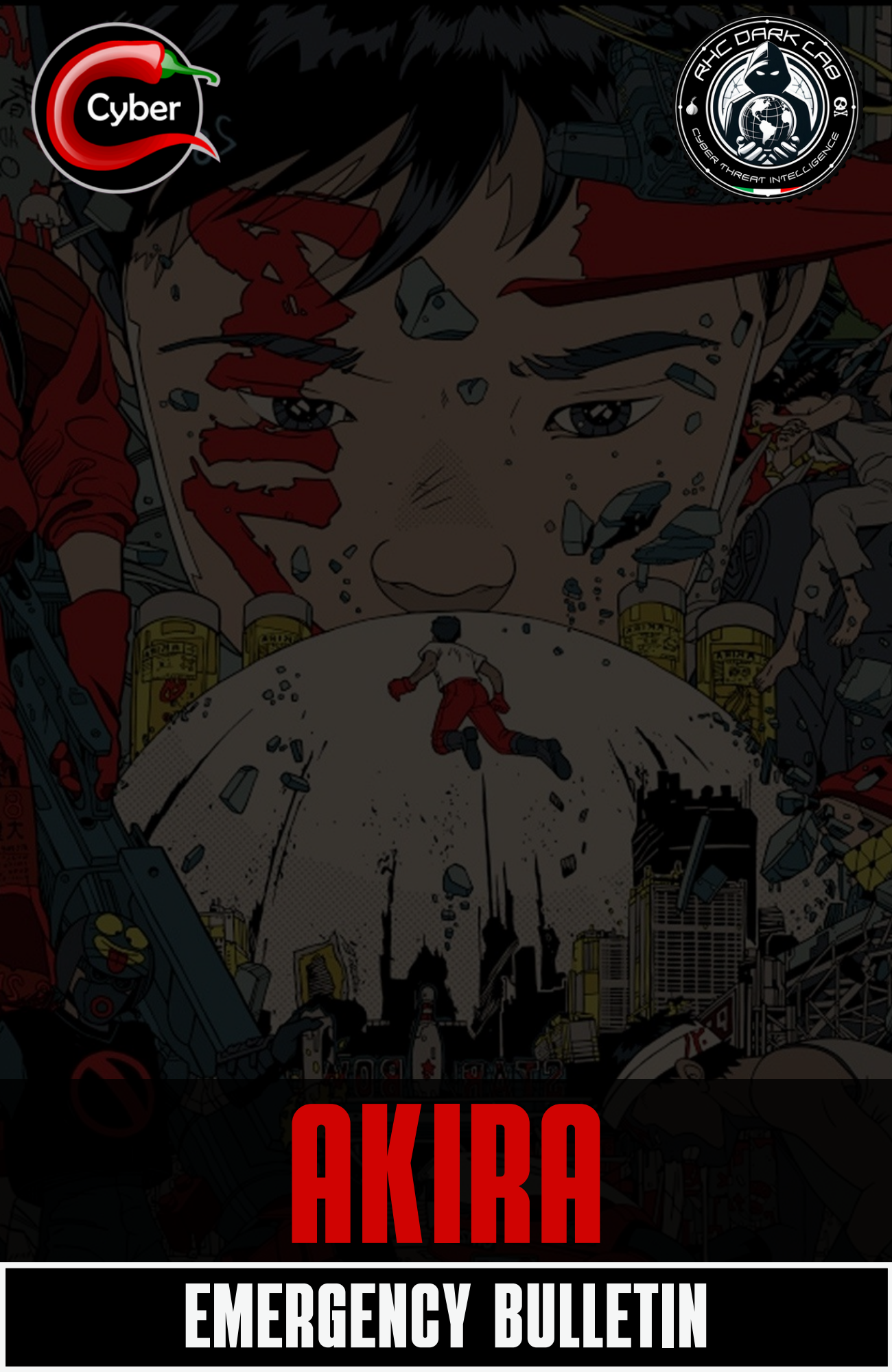
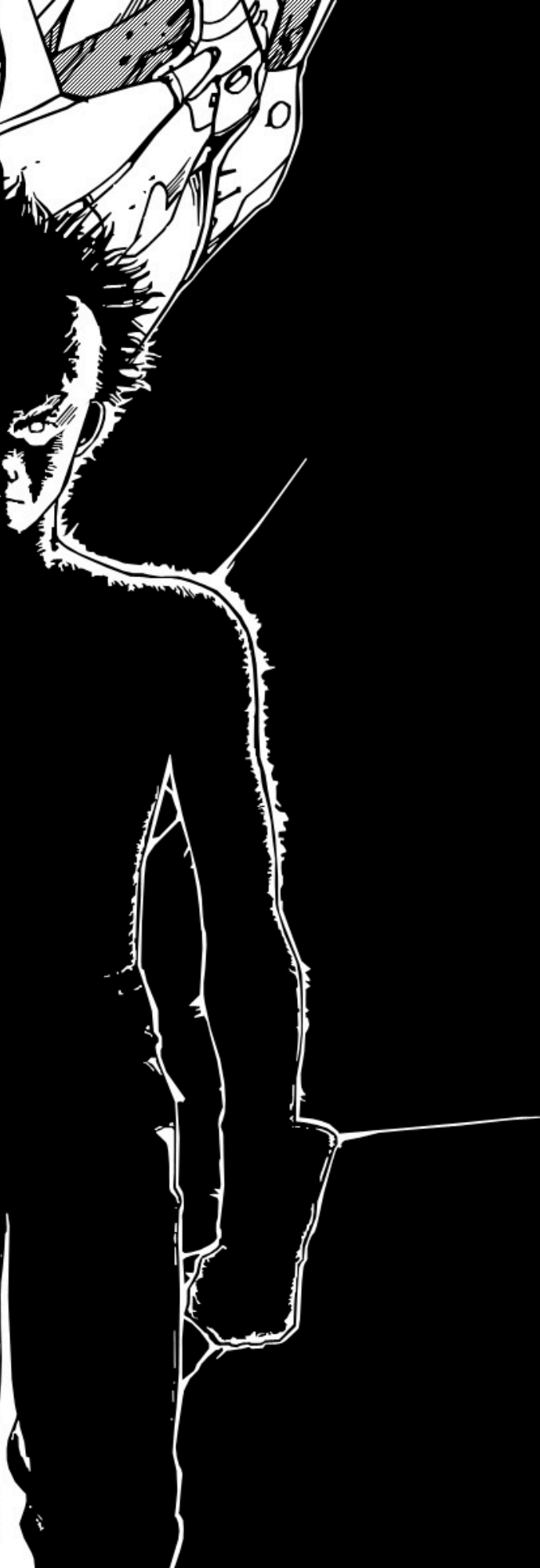




AKIRA

EMERGENCY BULLETIN



INDICE

I INTRO

A. CHI SIAMO

B. MOTIVAZIONI

C. AKIRA

I TTPs & MITIGAZIONI

A. BRUTED

B. TOOLS

C. MISC

I CONCLUSIONI

CHI SIAMO



RED HOT CYBER E' UN BLOG DI OPEN NEWS RIGUARDANTE IL MONDO DELLA SICUREZZA INFORMATICA, FONDATA NEL 2019 DA **MASSIMILIANO BROLI**. LA COMMUNITY DI RHC È COMPOSTA DA PROFESSIONISTI ED APPASSIONATI DEL SETTORE PIU' DISPARATI OFFRENDO UNA VISIONE INTERDISCIPLINARE.



DARK LAB È UN SOTTOGRUPPO DI RHC IDEATO E COORDINATO DA PIETRO MELILLO RIGUARDANTE LA CTI CON L'OBIETTIVO DI ENTRARE IN CONTATTO DIRETTO CON LE MINACCE ANALIZZANDONE I FUNZIONAMENTI. LE NOSTRE ATTIVITÀ OFFRONO ANALISI, REPORT ED INTERVISTE AI THREAT ACTORS.



AUTORI



ALESSIO STEFAN



BERNARDO SIMONETTO



FEDERICO MAZZOLINI

MOTIVAZIONI

NEL PERIODO CENTRALE DELLA PRIMA METÀ 2025 ABBIAMO OSSERVATO UNA SERIE DI ATTACCHI ALL'INTERNO DEL TERRITORIO ITALIANO RIVENDICATI DAL RAAS **AKIRA** CHE SEMBRA MUOVERSI SEMPRE DI PIÙ IN MANIERA MASSICCIA ALL'INTERNO DEL PAESE. DOPO UNA SERIE DI VITTIME NEL NORD-EST ITALIA E RECENTI ATTACCHI ABBIAMO DECISO DI PUBBLICARE QUESTO BULLETIN PER POTER DARE IL NOSTRO CONTRIBUTO ALLE ORGANIZZAZIONI CHE, SENSIBILIZZATE SUL TEMA, RICHIEDONO TUTTO IL SUPPORTO POSSIBILE PER POTER MIGLIORARE IL PROPRIO LIVELLO DI RESILIENZA DA MINACCE COME **AKIRA**.

NONOSTANTE IL FOCUS SU QUESTO SPECIFICO ATTORE NELLO SCENARIO RANSOMWARE TALE DOCUMENTO PUÒ ESSERE ESTESO A MINACCE ANALOGHE ADATTANDO I CONTENUTI ILLUSTRATI. I RECENTI MOVIMENTI DI QUESTO RAAS DEVONO SERVIRE DA OPPORTUNITÀ PER SENSIBILIZZARE SUL TEMA MIRANDO AD UN APPROCCIO PROATTIVO ALLA DIFESA PER LE RETI ITALIANE. **VISTA LA NATURA PERSISTENTE DI QUESTO TIPO DI MINACCE, LA RICHIESTA DI MIGLIORARE LA RESILIENZA E PREPARAZIONE AD ATTACCHI RANSOMWARE DEVE ESSERE SODDISFATTA NELLA MANIERA PIÙ EFFICIENTE POSSIBILE.**

SPERIAMO CHE QUESTO DOCUMENTO POSSA ESSERE UTILE NEI PROCESSI PER LA PROTEZIONE DELLE INFRASTRUTTURE. ABBIAMO RESO I CONTENUTI IL PIÙ ADERENTI POSSIBILE AD UNA VISIONE TECNICA CERCANDO DI BILANCIARE LA CONOSCENZA DEI METODI DI ATTACCO E LE TECNICHE DI MITIGAZIONE. SOTTOLINEAMO CHE I RISULTATI DELLE NOSTRE RICERCHE POSSONO RISULTARE PARZIALI E COERENTI CON IL MODELLO DELLA MINACCIA ATTUALE, **INVITIAMO I LETTORI AD INTEGRARE CON FONTI ALTERNATIVE E RIMANERE AGGIORNATI ATTRAVERSO CANALI DI INFORMAZIONE SPECIFICI.**



AKIRA

IL RANSOMWARE-AS-A-SERVICE **AKIRA** APPARE PER LA PRIMA VOLTA NEL MARZO DEL 2023 DOVE HA ALL'ATTIVO PIÙ DI **300 VITTIME** CON GUADAGNI (STIMATI) TRA I **\$60 MLN** ED **\$80 MLN** ESTORTI DOPO I LORO ATTACCHI. DOPO DIVERSI SMANTELLAMENTI E OPERAZIONI AI DANNI DI ALTRI GRUPPI RAAS, AKIRA HA RICEVUTO UN AUMENTO DEI SUOI AFFILIATI PORTANDO AD AUMENTARE LA INTENSITÀ DELLE LORO OPERAZIONI PORTANDOLO AL **PRIMO POSTO NELL'APRILE 2025 [16% DEGLI ATTACCHI GLOBALI]** PER NUMERO DI VITTIME. L'ORIGINE DEL GRUPPO È STATA ASSEGNATA AL GRUPPO **CONTI** GRAZIE ALLA UNIONE DI REVISIONI TECNICHE ED OSINT.



```
AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think of our actions as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow our instructions to get back to your daily routine, by cooperating with us you will minimize the damage that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extremely simple - enter the desired command in the input line and enjoy the juiciest information that corporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and cannot be traced to the place of final storage nor deleted by anyone besides us.

guest@akira:~$ help

List of all commands:

leaks      - hacked companies
news       - news about upcoming data releases
contact    - send us a message and we will contact you
help       - available commands
clear      - clear screen

guest@akira:~$
```

I SERVIZI RANSOMWARE DI AKIRA OFFRONO AI LORO AFFILIATI SUPPORTO PER **WINDOWS, ESXI E LINUX** PER POTER DANNEGGIARE IL PIÙ POSSIBILE LE RETI ALLE QUALE OTTENGONO ACCESSO. **GLI OPERATORI DEL RAAS SI SONO SOFISTICATI NEL TEMPO** PERMETTENDOLI DI OTTENERE L'ACCESSO INIZIALE SENZA L'USO DEL PHISHING O SIMILARI. OLTRE ALLE ABILITÀ TECNICHE DEI SUOI AFFILIATI, AKIRA RUBA DATI SENSIBILI PRIMA DI CIFRARE I FILE ALL'INTERNO DELLE MACCHINE PER POTER IMPLEMENTARE UNA **DOPPIA ESTORSIONE**. NELLE FASI DELLE OPERAZIONI DEL GRUPPO VIENE SPESO DEL TEMPO PER LA RICERCA E DISTRUZIONE DI POTENZIALI BACKUP SPINGENDO ULTERIORMENTE LE VITTIME AL PAGAMENTO. PER CONCLUDERE, **AKIRA È UNO DEI RAAS PIÙ ATTIVI ED EFFICACI NELLO SCENARIO RANSOMWARE GLOBALE.**

TTPS & MITIGAZIONI



BRUTED

IL LEAK DELLE CHAT [1] DI **BLACKBASTA** HA FATTO EMERGERE UNO STRUMENTO SVILUPPATO ED UTILIZZATO DAL RAAS PER AUTOMATIZZARE LA SCANSIONE E IL BRUTEFORCING DI DEVICE PERIMETRALI CHIAMATO **BRUTED**. IL TOOL È STATO DISCUSO DA RHC IN UN ARTICOLO AD HOC [2] CHE INVITIAMO A RECUPERARE PER CAPIRNE IL FUNZIONAMENTO. SECONDO LE NOSTRE OSSERVAZIONI UNITE AI CONTENUTI DELLE CHAT LEAKATE CHE MOSTRANO STRETTE RELAZIONI TRA OPERATORI DI **AKIRA** E **BLACKBASTA** [3] [4] CI PORTANO A CONCLUDERE CHE **AKIRA STIA USANDO IL TOOL BRUTED (ALTA CONFIDENZA)**. DA DELLE PRIME ANALISI SU ALCUNE VITTIME ITALIANE IMPATTATE DAL GRUPPO NON SONO EMERSE EVIDENZE DIRETTE DI BRUTEFORCING NE DI METODI ALTERNATIVI PER ACCESSO INIZIALE QUALE PHISHING O SFRUTTAMENTO DI VULNERABILITÀ SU DISPOSITIVI ESPOSTI ALLA RETE PUBBLICA. ABBIAMO AMPLIATO LA NOSTRA VISIONE COMUNICANDO CON ALTRE AZIENDE ATTACCATE CHE HANNO CONFERMATO DI AVERE EDGE DEVICES CHE RIENTRANO NELLA LISTA DI QUELLI TARGHETTATI DA **BRUTED**. IL TOOL OFFRE AGLI OPERATORI AUTOMAZIONE DALLA SCANSIONE DI MASSA FINO ALLE FASI DI BRUTEFORCE CON ROTAZIONE DI PROXY **SOCKS5**, **USER-AGENT CUSTOM** PER TIPO DI DEVICE, **SUBDOMAINS BRUTEFORCING** ED **ANALISI DI CERTIFICATI SSL** PER LA CREAZIONE DI PASSWORD LIST MIRATE [5][6].

LE SEGUENTI TECNOLOGIE RIENTRANO NEL RAGGIO D'AZIONE DEL TOOL

- **SONICWALL NETEXTENDER**
- **PALO ALTO GLOBALPROTECT**
- **CISCO ANYCONNECT**
- **FORTINET SSL VPN**
- **CITRIX NETSCALER**
- **MICROSOFT RDWEB**
- **WATCHGUARD SSL VPN**



UNA VOLTA CHE IL TOOL HA TROVATO LE CREDENZIALI CORRETTE, SALVA TALI CREDENZIALI IN UN FILE CON **NOTIFICA ALL'ATTACCANTE TRAMITE TELEGRAM ED ALTRE API ESTERNE.** SUCCESSIVAMENTE GLI OPERATORI UTILIZZANO MANUALMENTE LE CREDENZIALI OTTENUTE PER ACCEDERE ALL'INFRASTRUTTURA OTTENENDO **ACCESSO INIZIALE** DALLA QUALE POI ESEGUIRE LATERAL MOVEMENT, INSTALLARE ED UTILIZZARE MALWARE IN PREPARAZIONE ALL'ESECUZIONE RANSOMWARE. A SUPPORTARE LA NOSTRA TESI SONO STATI **LOG INERENTI LE SSL VPN DI UNA DELLE VITTIME ITALIANE IMPATTATE.** ANALISI NEI DUE GIORNI ANTECEDENTI ALL'ATTACCO DI LOG È BASTATO PER RICONDURRE A TALI INDIRIZZI IP :

- 141.98.80.134
- 141.98.80.144
- 45.227.255.84
- **46.161.27.99**

IN PARTICOLARE L'IP **46.161.27.99** APPARTIENE AD UNA **SOTTORETE NOTA DA NOVEMBRE 2024 E CITATA DA DIVERSE FONTI AUTOREVOLI TRA CUI CISA** IN UN LORO COMUNICATO RIGUARDO A **BLACKBASTA [7]**, LA SOTTORETE APPARTIENE A **AS43350 [8] (NFORCE, PAESI BASSI).** IL RIUTILIZZO DI HOSTING USATI DA BLACKBASTA IN UNA OPERAZIONE BRUTEFORCE DI AKIRA AUMENTA LA PROBABILITÀ DI RELAZIONI OPERATIVE TRA I DUE RAAS. **AGGIUNGIAMO CHE IN VIA IPOTETICA ANCHE OPERATORI DEL RANSOMWARE CACTUS POTREBBERO AVERE ACCESSO AL TOOL.** NONOSTANTE NON CI SIANO PROVE A RIGUARDO IL FATTO CHE ANCHE QUESTO GRUPPO AVESSSE RELAZIONI CON BLACKBASTA POTREBBE AVERE ACCESSO AL FRAMEWORK DI **BRUTED.**





DI SEGUITO RIPROPIAMO LA TABELLA CREATA DA **ECLECTICIQ** DOPO CHE HANNO ANALIZZATO IL TOOL AVENDO ACCESSO A PARTE DEI SERVER DEL FRAMEWORK [9]. QUESTI VALORI SONO SPECIFICI PER I TIPI DI DEVICE E POTREBBERO ESSERE CAMBIATI IN FUTURO DAGLI ATTACCANTI.

TI	Product	How It's Targeted	Key Detection Artifacts
0	Microsoft RDWeb	1) GET login.aspx → parse WorkspaceID 2) Post DomainUserName + UserPass 3) Check if redirected to default.aspx	Repeated POST to /RDWeb/Pages/login.aspx Param: DomainUserName, UserPass
1	Cisco AnyConnect (ASA)	1) Initial <config-auth> to fetch group options 2) Try group + user + password 3) Check for <session-id> in reply	- User-Agent: "AnyConnect Windows 4.4.02039" - <config-auth client="vpn" type="auth-reply">
2	SonicWall NetExtender	1) GET /cgi-bin/welcome + domain parse 2) Post domain=...&username=...&password=... 3) Check for swap= or X-NE-...	- User-Agent: "SonicWALL NetExtender for Windows 10.2.339" - cgi-bin/userLogin attempts
3	Fortinet SSL VPN	POST to /remote/logincheck Body: ajax=1&username=...&credential=... Success if ret=1, grpname=	- Repeated requests to /remote/logincheck - Checking ret=1, grpname= in the response
4	WatchGuard SSL VPN	1) GET landing page to parse auth-domain-list 2) POST to /?action=sstvpn_logon&fw_username=...&fw_password=...&fw_domain=...	- Param: fw_username, fw_password, fw_domain - Looks for <logon_status>1 in XML
5	Palo Alto GlobalProtect	1) GET/POST to /global-protect/getconfig.esp 2) Body includes clientgversion=6.0.7-372 3) Check for <policy> in XML	- User-Agent: "PAN GlobalProtect/6.0.7-372" - Path: /global-protect/getconfig.esp
6	Citrix Gateway	1) POST to /cgi/login 2) Body: login=<user>&passwd=<pass> 3) Success if NSC_AAAC or redirect to /cgi/setclient?wica	- User-Agent: "CitrixReceiver/23.11.1.41 Windows/10.0" - Checking NSC_AAAC= cookie

AD AGGIUNTA DI QUESTI ARTEFATTI PROPONIAMO LE SEGUENTI TECNICHE PER UNA POSTURA ROBUSTA ED EFFICACE COME RISPOSTA A **BRUTED**:

■ LOG POLICY

UNA **GESTIONE ROBUSTA ED EFFICIENTE** DEI LOG È UNO DEI METODI PRINCIPALI PER POTER USARE TOOL DI DETECTION E TRAFFIC ANALYSIS IN MANIERA EFFICACE. LA **RETENTION DEI LOG DEVE ESSERE SUFFICIENTE** A POTENZIALI INVESTIGAZIONI O PROCESSI DI INCIDENT RESPONSE.



MITIGAZIONI

■ MFA & PASSWORD/ACCESS POLICY

PER QUALSIASI PUNTO DI ACCESSO DA RETE PUBBLICA (EG:/ VPN, RDPWEB) DEVONO INTEGRARE MFA, IN PARTICOLARE SE I DEVICE RIENTRANO NELLA LISTA DEI TARGET USATI DA **BRUTED**. GLI ATTACCANTI COME **AKIRA** SONO CARATTERIZZATI DA UN ALTO GRADO DI ADATTABILITÀ E VISTA LA ATTENZIONE SULLE ORGANIZZAZIONI ITALIANE INVITIAMO AD IMPLEMENTARE MFA SU TUTTI GLI EDGE DEVICES PRESENTI.

SCONSIGLIAMO L'USO DI MFA TRAMITE SMS CHE POTREBBE ESSERE BYPASSATO DA ATTACCHI COME SIM SWAP O SOCIAL ENGINEERING. UN **CONTROLLO SUI TENTATIVI DI ACCESSO A LIVELLO DI ACCOUNT** ACCOMPAGNATO DA CORRELAZIONI TEMPORALI (EG:/ TENTATIVO/ACCESSO AL DI FUORI DELL'ORARIO LAVORATIVO) CON BLOCCO DEL PROFILO IN CASO DI POTENZIALE VIOLAZIONE SONO TECNICHE EFFICACI PER MITIGARE LA ROTATION DEGLI INDIRIZZI DI ORIGINE DELLE RICHIESTE. L'UTILIZZO DI **ACCOUNT HONEYPOT** CON PASSWORD [VOLUTAMENTE] DEBOLI POSSONO ESSERE INTEGRATI E MONITORATI PER POTER DISINCENTIVARE GLI SFORZI DEGLI ATTACCANTI BLOCCANDO GLI INDIRIZZI DI PROVENIENZA O REINDIRIZZANDO IN AMBIENTI SANDBOX. INFINE UNA FORTE PASSWORD POLICY DEVE ESSERE LA BASE PER LA PREVENZIONE AD **OPERAZIONI DI BRUTEFORCING**.

■ LEAST PRIVILEGE POLICY

GLI ACCOUNT PER ACCESSI VPN/FIREWALL/RDP DOVREBBERO AVERE SOLAMENTE I **PRIVILEGI NECESSARI** ALLE FUNZIONI RICHIESTE ALL'UTENTE ELIMINANDO ACCESSI O RUOLI CHE POTREBBERO ESSERE ABUSATI DAGLI ATTACCANTI PER PASSARE ALLE FASI SUCCESSIVE DEI LORO ATTACCHI.



MITIGAZIONI

■ PATCH MANAGEMENT

DARE PRIORITÀ AI DEVICE PERIMETRALI PER IL PATCH DI POTENZIALI VULNERABILITÀ IN ESSERE E FUTURE. DATO CHE IL FRAMEWORK DI **BRUTED** INCLUDE FUNZIONI DI SCANSIONE DI MASSA GLI OPERATORI POTREBBERO IMPLEMENTARE FILTRAGGIO PER VULNERABILITÀ CHE POSSONO ESSERE ABUSATE PER OTTENERE ACCESSO INIZIALE. MANTENERE I DEVICE ESPOSTI SEMPRE AGGIORNATI PERMETTE DI GIOCARE D'ANTICIPO RISPETTO AD ATTACCANTI CHE, COME **AKIRA**, FOCALIZZANO LA LORO ATTENZIONI SUL PERIMETRO DELLE ORGANIZZAZIONI. **ELIMINARE ACCOUNT DI DEFAULT E SERVIZI INUTILIZZATI** PER RIDURRE LA SUPERFICIE DI ATTACCO.

■ PIANI DI RISPOSTA

PREPARARE DIPENDENTI ED AMMINISTRATORI DI RETE NEI PROCESSI DI RISPOSTA QUANDO VIENE RILEVATO UN TENTATIVO DI BRUTEFORCING O DI ACCESSO ILLECITO. TRA I PROCESSI DEVONO ESSERE CHIARITE METODI DI PASSWORD RESET, ATTENENDOSI ALLA PASSWORD POLICY, PER ANNULARE GLI SFORZI DEGLI ATTACCANTI DOPO CHE HANNO OTTENUTO CREDENZIALI VALIDE.

IOC INDIVIDUATI

141.98.80.134

141.98.80.144

45.227.255.84

46.161.27.99

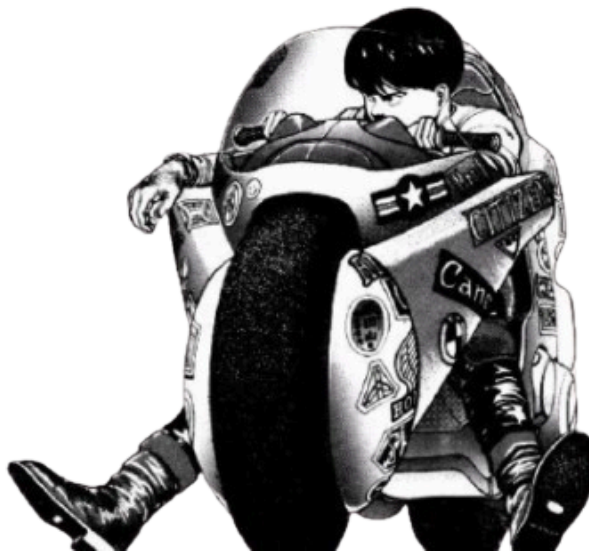
TOOLS



AKIRA È PARTICOLARMENTE VELOCE A RAGGIUNGERE LE FASI DI IMPATTO TRA ESFILTRAZIONE DI FILES ED ESECUZIONE DEL LORO RANSOMWARE, CON OPERAZIONI COMPLETATE IN MENO DI 24 ORE **[10]** DALL'ACCESSO INIZIALE RENDE SUPERFLUA LA NECESSITÀ DI PERSISTENZA EVITANDO DI LASCIARE TRACCE SULLE RETI COLPITE. NONOSTANTE LA VELOCITÀ E FURTIVITÀ DEGLI OPERATORI DIVERSE ANALISI ESTERNE SONO RISUCITE AD INDIVIDUARE LO STATO ATTUALE DEL GRUPPO E GLI STRUMENTI, IN QUESTA SEZIONE CERCHEREMO DI COPRIRE LE PRINCIPALI COMPONENTI OSSERVATE.

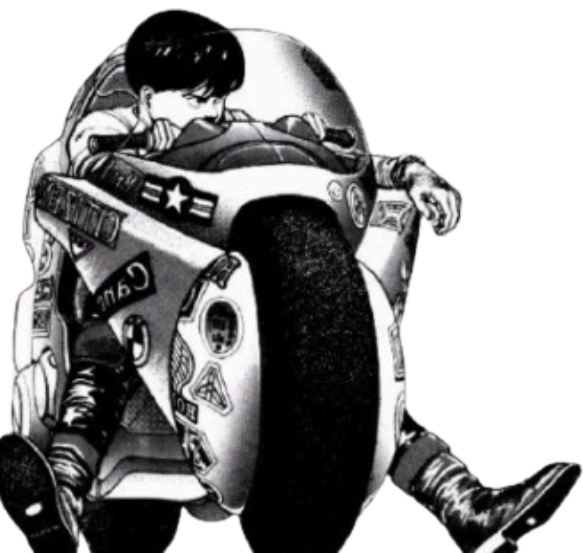
SHARPHOUND **[11]**

DATA COLLECTOR SCRITTO IN C# PER **BLOODHOUND** **[12]**, TOOL USATO PER LA VISUALIZZAZIONE DI ACCESSI/RELAZIONI/CONFIGURAZIONI IN AMBIENTI **ACTIVE DIRECTORY (AD)**. GRAZIE ALL'UTILIZZO DEI PROTOCOLLI **LDAP** E **SMB** VIENE SALVATO IN FORMATO JSON (COMPRESSO IN .ZIP) LO STATO DELLE DIVERSE COMPONENTI **AD** PER POTER POI ESSERE VISUALIZZATE TRAMITE GRAFI SEMPLIFICANDO LA SCOPERTA DI PERCORSI UTILI PER L'OTTENIMENTO DI ACCESSI NECESSARI ALLE OPERAZIONI DI ATTACCO. **LE RETI AD POSSONO CONTENERE PERCORSI INVOLONTARI** CHE POSSONO FARE OTTENERE PRIVILEGI INDESIDERATI SPECIALMENTE SU AMBIENTI COMPLESSI CON UN NUMERO MEDIO/ALTO DI OGGETTI (EG:/ COMPUTER, UTENTI, GPO). IL FRAMEWORK DI **BLOODHOUND** E RELATIVI **DATA COLLECTOR** SONO DISPONIBILI GRATUITAMENTE ED INVITIAMO LE ORGANIZZAZIONI AD UTILIZZARLI PER BENEFICIARE DEL TIPO DI VISIONE (SEMPLIFICATA) OFFERTA PERMETTENDO DI APPROFONDIRE LA CONOSCENZA DELLA RETE E DI RISOLVERE POTENZIALI PUNTI DI ABUSO.



PER POTER INDIVIDUARE L'USO DI **SHARPHOUND** È CONSIGLIABILE MONITORARE I SEGUENTI **EVENT ID** TRIGGERATI DAL TOOL, IMPORTANTE FILTRARE GLI ALERT PER EVITARE FALSI-POSITIVI CHE POTREBBERO CONFONDERE I SIEM O ALTRE SOLUZIONI DI MONITORAGGIO.

- **4648** - UTILIZZO DI CREDENZIALI DIFFERENTI DALL'UTENTE IN USO, COME AD ESEMPIO CHIAMATE DEL COMMANDO **RUNAS**.
- **5145** - ACCESSO A CONDIVISIONE DI RETE, IL DATA COLLECTOR ESEGUE (SE RICHiesto DALL'OPERATORE) UN ALTO NUMERO DI RICHIESTE SMB PER LA RACCOLTA INFORMAZIONI.
- **4662** - TRIGGER ABILITATO QUANDO UNA OPERAZIONE VIENE ESEGUITA SU UNO OGGETTO SPECIFICO. SELEZIONANDO SPECIFICHE COMPONENTI (TRA CUI QUELLE CRITICHE) ED ABILITANDO IL **SACL (SYSTEM ACCESS CONTROL LIST)** SI POSSONO RILEVARE TENTATIVI DI ENUMERATION DA PARTE DI MINACCE CON ACCESSO INTERNO.
- **257/258 (SYSMON)** - TRA I DATI COLLEZIONATI DAL COLLECTOR SONO PRESENTI I NOMI DELLE WORKSTATION INTERNE TRAMITE **DNS**, UN PICCO INSOLITO DI QUESTE QUERY DISTRIBUITE IN MANIERA ANOMALA SONO UN SEGNALE DA TENERE IN CONSIDERAZIONE
- **3 (SYSMON)** - SHARPHOUND EFFETTUA CONNESSIONI A PORTE 389/636 (LDAP/LDAPS) E 445 (SMB) VERSO I DOMAIN CONTROLLER E GLI HOST PRESENTI NELLO STESSO SEGMENTO DI RETE CREANDO UN VOLUME RILEVANTE DI QUESTE CONNESSIONI IN UN PERIODO DI TEMPO BREVE.

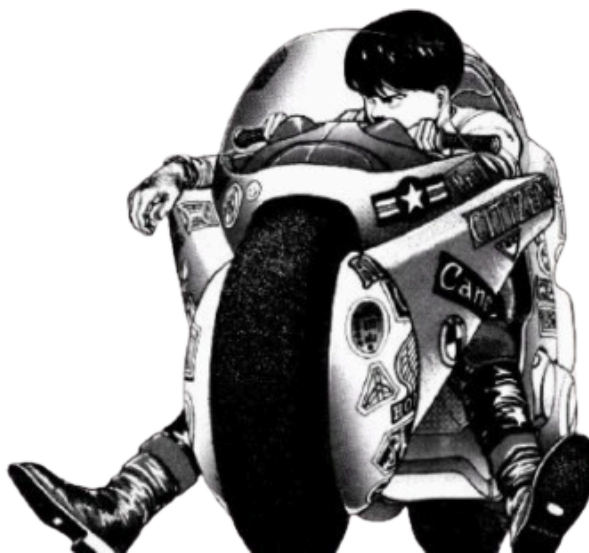


OLTRE AGLI EVENT ID DI WINDOWS LE **QUERY LDAP** POSSONO ESSERE MONITORATE TRAMITE **ETW** **[EVENT TRACING FOR WINDOWS]** AGGIUNGENDO GRANULARITÀ E PRECISIONE. I COLLECTOR DI BLOODHOUND USANO IN MANIERA ESTENSIVA IL FILTRO **"SAMACCOUNTTYPE="** AD ESEMPIO PER OTTENERE TUTTI GLI USER CON **[SAMACCOUNTTYPE=805306368]** E COMPUTER CON **[SAMACCOUNTTYPE=805306369]**. SEMPRE CON IL SUPPORTO DI **ETW** SI POSSONO TRACCIARE LE CHIAMATE ALLE API COME **NETSESSIONENUM** E **NETWKSTAUSERENUM** USATE NELLA FASE DI ENUMERATION.

INFINE CREARE **OGGETTI-ESCA** VISIBILI SOLAMENTE TRAMITE **LDAP** DONA UN SUPPORTO NOTEVOLE CHE, CORRELATO A QUANTO ESPRESSO SOPRA, INSERISCE UN LIVELLO DI CONFIDENZA MAGGIORE PER RILEVAZIONE E RISPOSTA A **SHARPHOUND**.

RISORSE UTILI

- **SNIFFING OUT SHARPHOUND ON ITS HUNT FOR DOMAIN ADMIN** **[13]**
- **SHARPHOUND DOCUMENTATION** **[14]**
- **BLOODHOUND COLLECTORS CHEATSHET** **[15]**
- **SHARPHOUND DETECTION** **[16]**
- **IMPLEMENTAZIONE SACL SU OGGETTI AD** **[17]**
- **CONFIGURAZIONE ETW** **[18]**

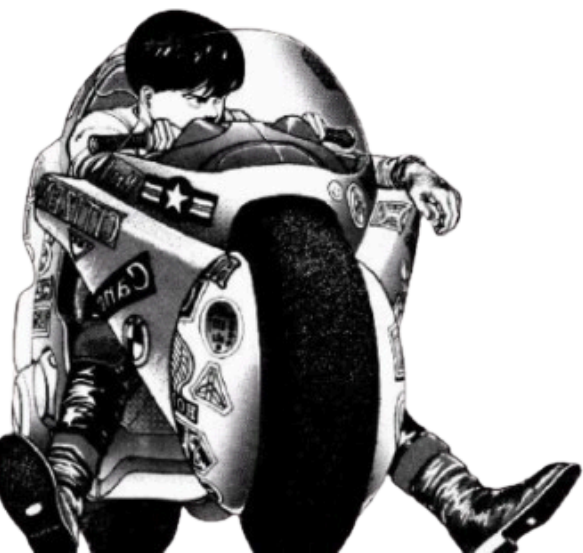


COMSVCS.DLL

LE TECNICHE “**LIVING OFF THE LAND**” (**LOL**) USANO BINARI O LIBRERIE DLL PRESENTI NEL SISTEMA OPERATIVO E QUINDI CONSIDERATI LEGGITTIMI OLTRE CHE SIGNED DA MICROSOFT NEL CASO DI WINDOWS OS. ABUSARE DI COMPONENTI INTERNE SEMPLIFICA L’EVASIONE ALLE SOLUZIONI TRADIZIONALI PER LA SICUREZZA DEGLI ENDPOINT. SONO MOLTEPLICI LE TATTICHE CHE POSSONO ESSERE RAGGIUNTE DAI DIVERSI **LOL** MA NEL CASO DI **AKIRA** SI È NOTATO UN PERSISTENTE USO DI **COMSVCS.DLL** PER ESEGUIRE UN DUMP DI **NTDS.DIT**, FILE PRESENTE NEI **DOMAIN CONTROLLER** CONTENENTE GLI HASH DEGLI UTENTI DELLA RETE **AD**, E MEMORIA DEL PROCESSO **LSASS** CONTENENTE CREDENZIALI DI UTENTI (AUTENTICATI) A LIVELLO WORKSTATION. UN USO COMUNE DI QUESTA DLL È DI ESEGUIRLA TRAMITE UN ESEGUIBILE **LOL** PRESENTE SU WINDOWS PER POTER ESEGUIRE FUNZIONI SPECIFICHE ALL’INTERNO DELLA LIBRERIA, **RUNDLL32**.

RUNDLL32 C:\WINDOWS\SYSTEM32\COMSVCS.DLL MINIDUMP [PID] [OUTPUT] FULL

IN PRIMO LUOGO BISOGNA IRROBUSTIRE LA RETE E LE SINGOLE WORKSTATION PER EVITARE CHE VENGANO OTTENUTI ACCESSI AMMINISTRATORE (DI RETE/LOCALE) CHE RIMANE L’UNICO REQUISITO PER POTER INTERAGIRE CON **NTDS.DIT** E IL PROCESSO **LSASS**. IN AGGIUNTA MONITORARE L’USO DI **COMSVCS.DLL** IN COMBINAZIONE CON **RUNDLL32.EXE** ANCHE DA UTENTI CON ACCESSO DA AMMINISTRATORI È UN OTTIMO TRIGGER PER RIVELARE AZIONI MALEVOLE. L’**EVENT ID 7 (IMAGE CREATION, SYSMON)** SULLA DLL CON TALE FILTRO ED ALTRI PROCESSI INSOLITI FA DA SUPPORTO A QUESTA REGOLA DI DETECTION.



VISIONARE L'USO DI **COMSVCS.DLL** NON RISULTA ESSERE UNA SCELTA EFFICACE VISTO L'ALTO NUMERO DI FALSI POSITIVI CHE POTREBBERO EMERGERE ESSENDO UNA COMPONENTE USATA E GESTITA IN PRIMO LUOGO DAL SISTEMA OPERATIVO E PROGRAMMI LEGITI. PER COMPENSARE TALE SVANTAGGIO CI SI PUÒ CONCENTRARE SU 2 SPECIFICI **EVENT ID**:

- **10 (SYSMON)** = TENTATIVI DI ACCESSO A PROCESSI **LSASS.EXE** (SOLITAMENTE CON **PID** DI VALORE BASSO) DA PROCESSI NON DI SISTEMA SONO UN FORTE SEGNALE DI ABUSO RENDENDO SUFFICIENTE UNA IMPLEMENTAZIONE DI MONITORAGGIO SU QUESTO SPECIFICO EVENT ID.
- **4656** = IL TRIGGER DI QUESTO EVENT ID È LA APERTURA DI UN HANDLE SU UN OGGETTO, COME FILE **NTDS.DIT**. ASSIEME A QUESTO SI PUÒ INTEGRARE ANCHE L'ID **4663** PER UN QUALSIASI ACCESSO AL FILE ATTENZIONATO. COME LSASS.EXE ANCHE NTDS.DIT NON DOVREBBE ESSERE SOGGETTO DI INTERAZIONE DA UTENTI/PROCESSI NON DI SISTEMA.

SYSMON PRENDE UN RUOLO INDISPENSABILE OFFRENDO UNA VISIONE GRANULARE SU OPERAZIONI EFFETTUATE NELLE WORKSTATION NECESSARIA PER L'ESECUZIONE DI TECNICHE **LOL**. VISTO LA NATURA SENSIBILE DEL FILE/PROCESSO PRESO DI MIRA DAGLI ATTACCANTI L'IMPLEMENTAZIONI DI **SOAR** POSSONO IMPLEMENTARE LA DISABILITAZIONE DELL'ACCOUNT CHE HA ORIGINATO LA RICHIESTA OLTRE A NOTIFICARE GLI AMMINISTRATORE DI RETE.

RISORSE UTILI

- **COMSVCS.DLL LOLBAS [19]**
- **DETECTING AND PREVENTING LSASS CREDENTIAL DUMPING ATTACKS [20]**
- **CREDENTIAL DUMPING: LSASS MEMORY DUMP DETECTION [21]**
- **CREDENTIAL DUMPING: NTDS.DIT DUMP DETECTION [22]**
- **NTDS.DIT AND CREDENTIAL DUMPING [23]**



EXFILTRATION

I TOOL **FILEZILLA**, **RCLONE** E **WINSXP** ASSIEME A **WINRAR** SONO I PRINCIPALI VETTORI PER IL FURTO DI DATI DA PARTE DI **AKIRA** NELLE FASI ANTECEDENTI ALLA CIFRATURA. LA SCELTA DI STRUMENTI LEGITTIMI PERMETTONO DI EVITARE RILEVAZIONE DA PARTE DI **ANTI-VIRUS** ED **EDR** RENDENDO POSSIBILE LA PREVENZIONE SOLO CON SPECIFICI CONTROLLI SU QUESTI TOOL. LA PROTEZIONE DA TATTICHE DI EXFILTRATION TUTELA LE ORGANIZZAZIONE DA PRESSIONI AGGIUNTIVE IN FASE DI NEGOZIAZIONE DA PARTE DI **AKIRA** O ALTRI RAAS CHE IMPLEMENTANO LA **DOPPIA ESTORSIONE** NELLE LORO OPERAZIONI.

- **APPLOCKER** È UNA SOLUZIONE DIRETTA ED EFFICACE PER LIMITARE L'USO DI APPLICAZIONI LEGITE CHE NON VENGONO CONSIDERATE NECESSARIE DALLA ORGANIZZAZIONE. TRAMITE WHITELISTING SI LIMITA L'ESECUZIONE DI ESEGUIBILI COME QUELLI SOPRA CITATI MA ANCHE PER PROGRAMMI **RDP** ESTENSIVAMENTE USATI DAGLI ATTACCANTI RANSOMWARE.
- SOLUZIONI **DLP (DATA LOSS PROTECTION)** PER BLOCCARE TENTATIVI DI FURTO IN BASE AL CONTENUTO O AL CONTESTO DI ESECUZIONE. DESTINAZIONI A SERVIZI CLOUD COME GOOGLE, MEGA E SIMILARI VENGONO INDIVIDUATI E BLOCCATI.
- **MONITORAGGIO DEL TRAFFICO IN USCITA** DEVE ESSERE UNA PRATICA COMUNE CON UN BILANCIAMENTO TRA ANALISI AUTOMATICHE E MANUALI PER POTER INDIVIDUARE L'ORIGINE DEL FURTO E FAR PARTIRE I PROCESSI DI CONTENIMENTO

RISORSE UTILI

- DETECT AND PREVENT COMMON DATA EXFILTRATION ATTACKS [24]
- DETECTING RCLONE [25]
- COMMON DATA-EXFILTRATION TOOLS [26]

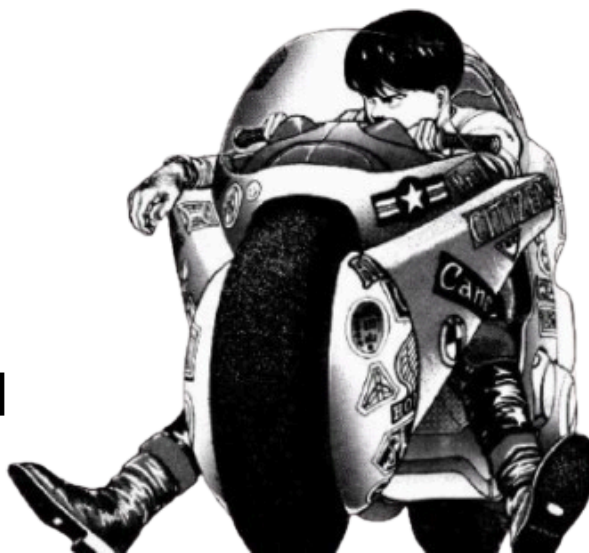


BRING-YOUR-OWN-DRIVER (BYOVD) È UNA TECNICA CHE SFRUTTA LE FRIME DIGITALI DI DRIVER VULNERABILI CHE POSSONO PORTARE A **PRIVILEGE ESCALATION, BLOCCO DI PROCESSI PROTETTI** O ALTRE OPERAZIONI RESE POSSIBILI DEL CONTESTO KERNEL NELLA QUALE IL DRIVER VIENE LOCALIZZATO UNA VOLTA INSERITO NEL SISTEMA. AKIRA ERA STATO OSSERVATO USARE UNA VERSIONE MODIFICATA DI **TERMINATOR** [27] NEL 2024 E 2025 CHE UTILIZZA UNA VERSIONE VULNERABILE DI **ZAMGUARD64.SYS (ZEMANA ANTI-MALWARE)** [28]. IL TOOL RIESCE A FERMARE PROCESSI PROTETTI DI SISTEMI COME AV, EDR ED ALTRE SOLUZIONI DI SICUREZZA. UNA VOLTA INSTALLATO IL DRIVER DIVENTA DIFFICILE IDENTIFICARE AZIONI MALEVOLE CON SOLUZIONI TRADIZIONALI VISTO CHE LE AZIONI A LIVELLO KERNEL VENGONO CONSIDERATE TRUSTED BY DEFAULT, I PRINCIPALI METODI DI MITIGAZIONI CHE PROPONIAMO SONO :

- WHITELISTING DEI DRIVER INSTALLATI TRAMITE **WDAC (WINDOWS DEFENDER APPLICATION CONTROL)** MANTENENDO VALIDI SOLO I DRIVER STRETTAMENTE NECESSARI ED EVITARE INSTALLAZIONE DI QUELLI NON PRESENTI NELLA LISTA ANCHE SE SIGNED.
- **AGGIORNAMENTO DI TUTTI I DRIVER INSTALLATI** (SPECIALMENTE DI ANTI-VIRUS ED EDR) PER EVITARE L'ABUSO DI DRIVER INSTALLATI CHE POTREBBERO CONTENERE VULNERABILITÀ ABUSABILI DAGLI ATTACCANTI.
- MONITORAGGIO **EVENT ID 6 (DRIVER LOADED, SYSMON)** UNITO ALLA CORRELAZIONE DI PATH INSOLITI O HASH SCONOSCIUTI.

RISORSE UTILI

- **LOLDRIVERS** [27]
- **APP CONTROL POLICY FOR BYOVD** [28]
- **STRATEGIES FOR VULNERABLE DRIVER ATTACKS** [29]



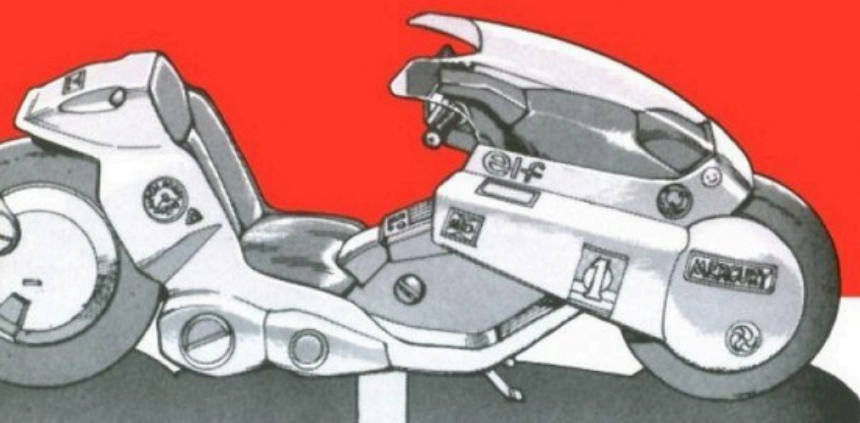
MISC III

I TOOL COPERTI NELLA SEZIONE PRECEDENTE NON DEVE CONSIDERARSI UNA LISTA COMPLETA E SUGGERIAMO DI RIMANERE AGGIORNATI SUI MOVIMENTI DEL GRUPPO NEL FUTURO PER POTERSI ADEGUARE MANTENENDO UN APPROCCIO PROATTIVO ALLA PROTEZIONE DEGLI ASSET ORGANIZZATIVI. DI SEGUITO VORREMMO ESPORRE DELLE LINEE GUIDE AGGIUNTIVE DA POTER APPORRE ALLE PROPRIE RETI PER RIDURRE L'IMPATTO DALLE MINACCE RANSOMWARE CHE, SECONDO LE NOSTRE ANALISI, CONTINUANO AD AUMENTARE ALL'INTERNO DEI CONFINI DEL BEL PAESE.

GESTIONE DEI PRIVILEGI

1

LE RETI ACTIVE DIRECTORY DEVONO ESSERE REVISIONATE E MODIFICATE SEGUENDO IL **TIERED ADMINISTRATION MODEL** [30][31] PER OTTENERE UNA VISIONE E GESTIONE SEMPLIFICATA DELLA SICUREZZA INTERNA. L'IMPLEMENTAZIONE DI POLICY **JUST-IN-TIME** [32][33] PERMETTONO DI OTTENERE, QUANDO NECESSARIO, I PRIVILEGI SOLO PER IL TEMPO NECESSARIO EVITANDO DI LASCIARE ESPOSTE SESSIONI AD ALTA INTEGRITA CHE POSSONO ESSERE ABUSATE DA ATTORI CON ACCESSO INTERNO



GESTIONE DEI BACKUP

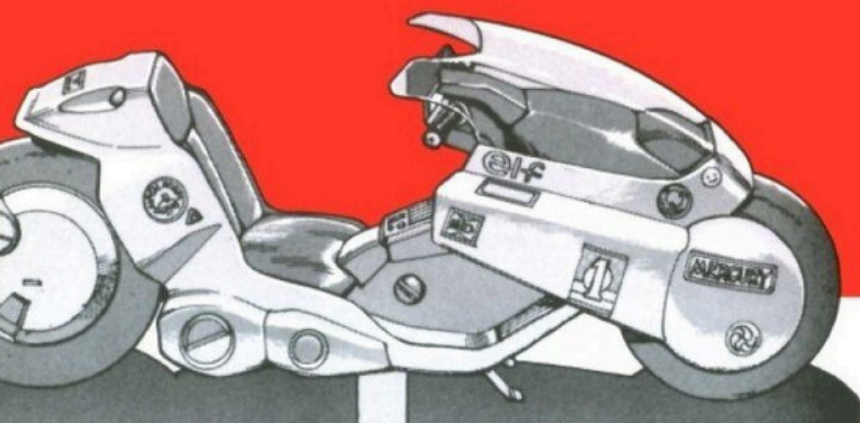
IL DANNO DEL RANSOMWARE È LA COMPROMISSIONE DEI DATI CHE SPESSO SI TRADUCE IN UN BLOCCO DELLE ATTIVITÀ DELLA AZIENDA IMPATTATA. SEGUIRE LA **REGOLA 3-2-1** (3 COPIE SU 2 MEDIA DIFFERENTI DI CUI 1 OFF-SITE) PER I DATI DEVE ESSERE LA BASE PER POTER RIPRISTINARE LE ATTIVITÀ. GLI ATTACCANTI SI SONO ADATTATI E SPESSO RICERCANO TALI BACKUP PER DISTRUGGERLI, I BACKUP DEVONO ESSERE PROTETTI TRAMITE **AIR GAP LOGICI**, **IMMUTIBILITÀ** ED ALTRI METODI.

2

ESXi HARDENING

LE INVESTIGAZIONI HANNO CONFERMATO COME **AKIRA** PRENDA DI MIRA I SISTEMI **ESXi** NELLE SUE OPERAZIONI. UNA **SEGMENTAZIONE EFFICACE DELLE VLAN** ASSIEME A **JUMBOX** PER LIMITARE L'ACCESSO DIRETTO E/O L'USO DELLA **MODALITÀ LOCKDOWN** PER ACCESSO ESCLUSIVO TRAMITE VCENTER SPHERE SONO SEMPLICI ACCORGIMENTI CHE MITIGANO LA COMPROMISSIONE DI QUESTO TIPO DI ASSET. POLICY DI LOG E BACKUP DEVONO INCLUDERE ESXi PER I PROCESSI DI MONITORAGGIO.

3



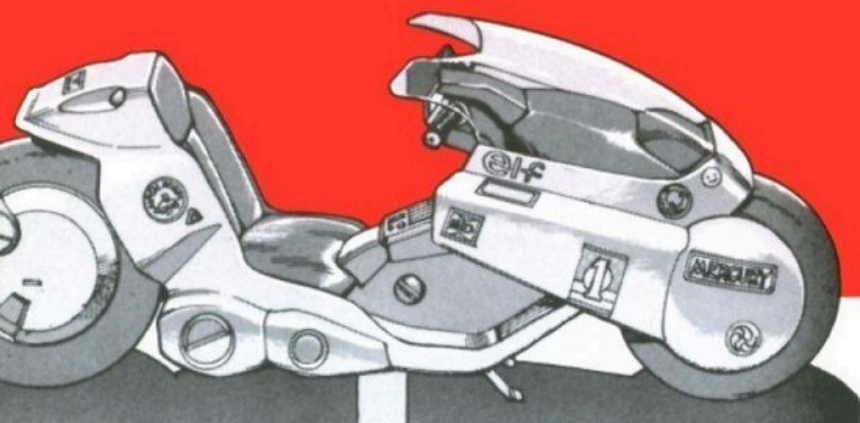
PROCESSI DI RECUPERO E RIPRISTINO

PER MANTENERE ALTA LA PREPARAZIONE DEL TEAM RESPONSABILE NELLA RISPOSTA DI
ATTACCHI COME QUELLO RANSOMWARE POSSONO ESSERE ESEGUITE DELLE
SIMULAZIONI PER VALUTARNE L'EFFICACIA E IL TEMPO D'ESECUZIONE. NON BASTA
LIMITARSI A PREDISPORRE DELLE LINEE GUIDE PURAMENTE TEORICHE MA TRAMITE IL
TESTING DI QUEST'ULTIME POSSONO ESSERE RIVALUTATE ED ADATTATE ALL'AMBIENTE.

4

CONSIDERAZIONE DEL RISCHIO

5 SPESSO SI TENDE A PENSARE CHE GLI ATTACCHI RANSOMWARE SIANO UNA MINACCIA
PER LE GRANDI AZIENDE O SETTORI SPECIFICI COME QUELLO GOVERNATIVO. IN REALTÀ
LA MAGGIOR PARTE DEGLI ATTACCHI RANSOMWARE TENDE A FOCALIZZARSI SULLE
MEDIE/PICCOLE AZIENDE OLTRE A QUELLE GRANDI, LE ORGANIZZAZIONI DEVONO
CONSIDERARE E VALUTARE L'INVESTIMENTO IN SICUREZZA INFORMATICA CERCANDO
SOLUZIONI ADATTE AL LORO AMBIENTE E BUDGET.



CONCLUSIONI

I RECENTI MOVIMENTI NEL (NORD) ITALIA CAUSATI DA **AKIRA** CI HANNO PORTATO PORTATO ALLA REDAZIONE DI QUESTO REPORT PER POTER CONDIVIDERE LA RELAZIONE TRA IL GRUPPO ED IL TOOL **BRUTED** SVILUPPATO DA **BLACKBASTA**. GRAZIE ALLE ANALISI DELLE CHAT LEAKATE E ANALISI FATTE DA TERZE PARTI POSSIAMO CONCLUDERE L'IPOTESI DELL'UTILIZZO DI **BRUTED** DA PARTE DI **AKIRA** IN TERRITORIO ITALIANO SIA SOSTENIBILE CON **ALTA CONFIDENZA**. SPERIAMO CHE LA CONDIVISIONE DI QUESTE PRIME SCOPERTE POSSANO SUPPORTARE ALTRE REALTÀ CHE SI OCCUPANO DEL MONITORAGGIO DELLE MINACCE.

VISTA LA DENSITÀ DI VITTIME ITALIANE ABBIAMO VOLUTO INTEGRARE LE NOSTRE SCOPERTE CON DELL LINEE GUIDE CHE POSSONO AIUTARE LE ORGANIZZAZIONI A MIGLIORARE LA PROPRIA POSTURA DI SICUREZZA PER CONTRASTARE **AKIRA**. I CONSIGLI PROPOSTI SONO DA PRENDERE COME INTRODUTTIVI, VALUTATI IN BASE ALLE ESIGENZE INTERNE ED INTEGRATI CON CONSULENZE PROFESSIONALI.

REDHOTCYBER ED IL SOTTOGRUPPO **DARKLAB** RIMANGONO APERTI PER EVENTUALI CHIARIMENTI, COLLABORAZIONI E PER CHIUNQUE VOLESSE INTEGRARE CON INFORMAZIONI AGGIUNTIVE PER IL SUPPORTO DELLE NOSTRE ANALISI.

