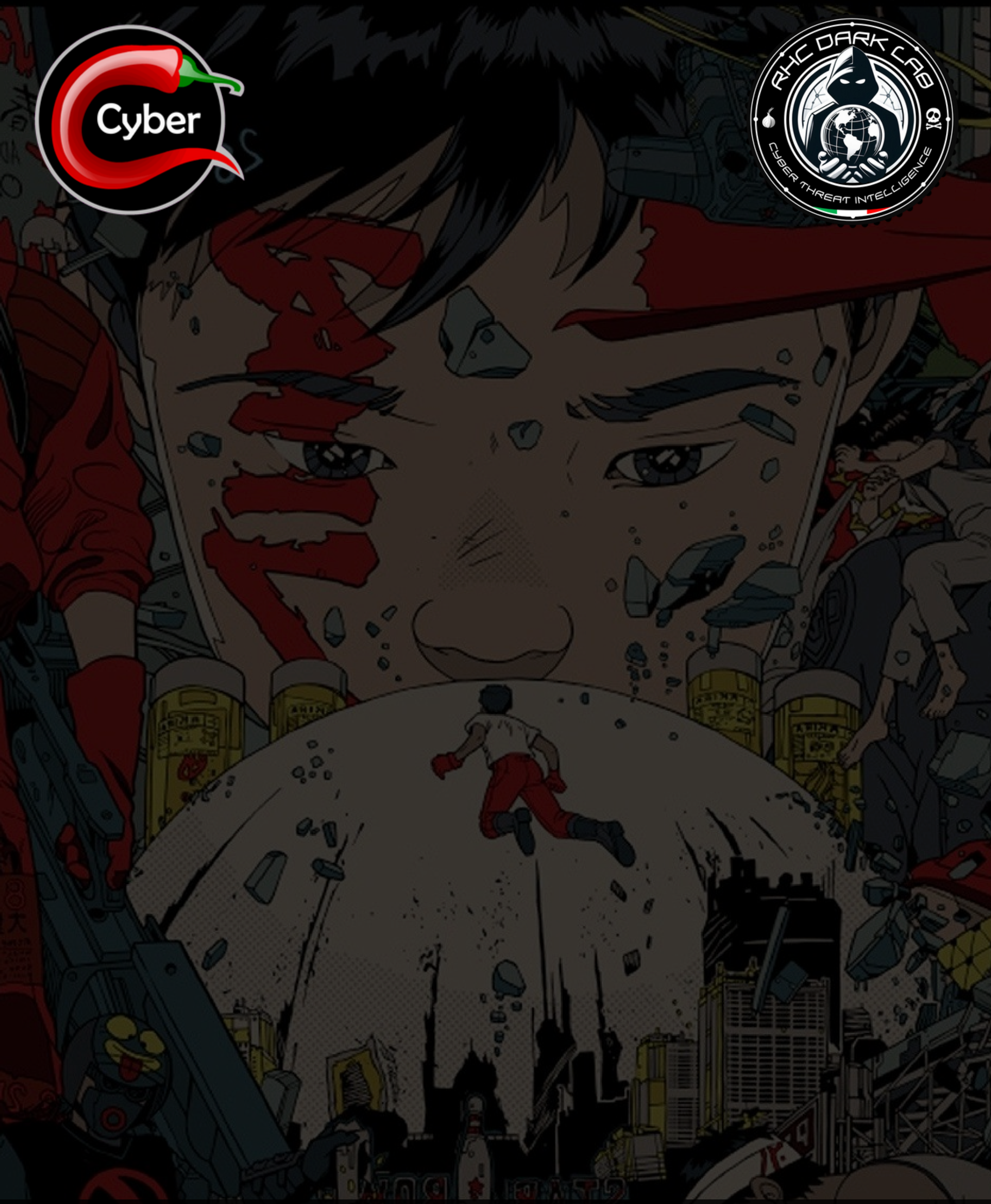
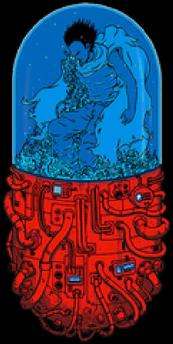


AKIRA

EMERGENCY BULLETIN

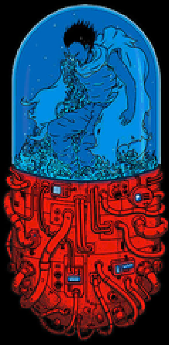
INDEX

ABOUT US



RED HOT CYBER IS AN OPEN NEWS BLOG REGARDING THE WORLD OF CYBER SECURITY, FOUNDED IN 2019 BY MASSIMILIANO BROLLI. THE RHC COMMUNITY IS COMPOSED OF PROFESSIONALS AND ENTHUSIASTS FROM THE MOST DIVERSE FIELD OFFERING AN INTERDISCIPLINARY VIEW.

DARK LAB IS A SUBGROUP OF RHC CONCEIVED AND COORDINATED BY PIETRO MELILLO CONCERNING CTI WITH THE GOAL OF GETTING IN DIRECT CONTACT WITH THREATS BY ANALYZING THEIR OPERATIONS. OUR ACTIVITIES OFFER ANALYSIS, REPORTS AND INTERVIEWS WITH THREAT ACTORS.



AUTHORS

ALESSIO STEFAN

BERNARDO SIMONETTO

FEDERICO MAZZOLINI

MOTIVATIONS

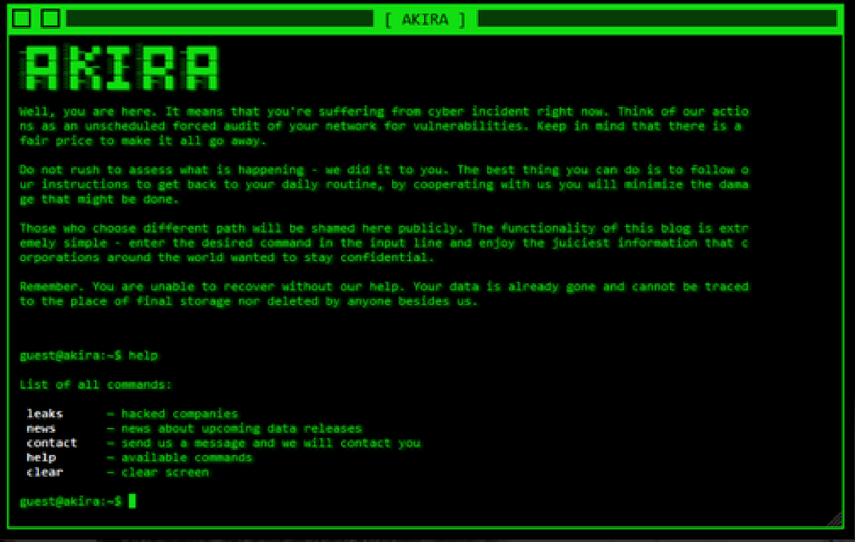
IN THE CENTRAL PERIOD OF THE FIRST HALF OF 2025 WE HAVE OBSERVED A SERIES OF ATTACKS INSIDE THE ITALIAN TERRITORY ATTRIBUTED BY THE RAAS AKIRA THAT SEEMS TO BE MOVING MORE AND MORE MASSICALLY INSIDE THE COUNTRY. AFTER A SERIES OF CASUALTIES IN NORTHEAST ITALY AND RECENT ATTACKS, WE DECIDED TO PUBLISH THIS BULLETIN IN ORDER TO BE ABLE TO GIVE OUR INPUT TO ORGANIZATIONS THAT, SENSITIZED TO THE ISSUE, REQUIRE ALL THE SUPPORT THEY CAN GET IN ORDER TO IMPROVE THEIR LEVEL OF RESILIENCE FROM THREATS LIKE AKIRA.

DESPITE THE FOCUS ON THIS SPECIFIC ACTOR IN THE RANSOMWARE SCENARIO THIS PAPER CAN BE EXTENDED TO SIMILAR THREATS BY ADAPTING THE CONTENTS ILLUSTRATED. RECENT MOVEMENTS OF THIS RAAS MUST SERVE AS AN OPPORTUNITY TO SENSITIZE ON THE ISSUE AIMING AT A PROACTIVE APPROACH TO DEFENSE FOR ITALIAN NETWORKS. GIVEN THE PERSISTENT NATURE OF THESE TYPES OF THREATS, THE DEMAND TO IMPROVE RESILIENCE AND PREPAREDNESS FOR RANSOMWARE ATTACKS MUST BE MET IN THE MOST EFFICIENT MANNER POSSIBLE.

WE HOPE THAT THIS DOCUMENT WILL BE USEFUL IN PROCESSES FOR INFRASTRUCTURE PROTECTION. WE HAVE MADE THE CONTENTS AS CLOSE TO A TECHNICAL VIEW AS POSSIBLE BY TRYING TO BALANCE KNOWLEDGE OF ATTACK METHODS AND MITIGATION TECHNIQUES. WE EMPHASIZE THAT THE RESULTS OF OUR RESEARCH MAY BE BIASED AND CONSISTENT WITH THE CURRENT THREAT MODEL, WE ENCOURAGE READERS TO SUPPLEMENT WITH ALTERNATIVE SOURCES AND STAY UPDATED THROUGH SPECIFIC INFORMATION CHANNELS.

AKIRA

THE RANSOMAWRE-AS-A-SERVICE AKIRA APPEARS FOR THE FIRST TIME IN MARCH 2023 WHERE IT HAS MORE THAN 300 VICTIMS AT STAKE WITH EARNINGS (ESTIMATED) BETWEEN $60 MLN AND $80 MLN EXTORTED AFTER THEIR ATTACKS. AFTER SEVERAL DISMANTLEMENTS AND OPERATIONS AGAINST OTHER RAAS GROUPS, AKIRA RECEIVED AN INCREASE IN ITS AFFILIATES LEADING TO AN INCREASE IN THE INTENSITY OF THEIR OPERATIONS BRINGING IT TO FIRST PLACE IN APRIL 2025 (16% OF GLOBAL ATTACKS) BY NUMBER OF VICTIMS. THE ORIGIN OF THE GROUP WAS ASSIGNED TO THE CONTI GROUP THROUGH THE UNION OF TECHNICAL AND OSINT REVIEWS.



```
Well, you are here. It means that you're suffering from cyber incident right now. Think of our actio
ns 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 o
ur instructions to get back to your daily routine, by cooperating with us you will minimize the dama
ge that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extr
emely simple - enter the desired command in the input line and enjoy the juiciest information that c
orporations 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:~$ █
```

AKIRA RANSOMWARE SERVICES OFFER THEIR AFFILIATES SUPPORT FOR WINDOWS, ESXI, AND LINUX IN ORDER TO DO AS MUCH DAMAGE AS POSSIBLE TO THE NETWORKS TO WHICH THEY GAIN ACCESS. RAAS OPERATORS HAVE BECOME SOPHISTICATED OVER TIME ALLOWING THEM TO GAIN INITIAL ACCESS WITHOUT THE USE OF PHISHING OR SIMILAR. IN ADDITION TO THE TECHNICAL SKILLS OF ITS AFFILIATES, AKIRA STEALS SENSITIVE DATA BEFORE ENCRYPTING FILES WITHIN THE MACHINES IN ORDER TO IMPLEMENT DOUBLE EXTORTION. IN THE STAGES OF THE GROUP'S OPERATIONS, TIME IS SPENT SEARCHING FOR AND DESTROYING POTENTIAL BACKUPS FURTHER PUSHING VICTIMS TO PAYMENT. IN CONCLUSION, AKIRA IS ONE OF THE MOST ACTIVE AND EFFECTIVE RAAS IN THE GLOBAL RANSOMWARE SCENARIO.

TTPS & MITIGATIONS

BRUTED

THE LEAK OF BLACKBASTA CHATS [1] BROUGHT TO LIGHT A TOOL DEVELOPED AND USED BY RAAS TO AUTOMATE THE SCANNING AND BRUTEFORCING OF PERIMETER DEVICES CALLED BRUTED. THE TOOL WAS COVERED BY RHC IN AN AD HOC ARTICLE [2] THAT WE INVITE YOU TO RECOVER TO UNDERSTAND HOW IT WORKS. ACCORDING TO OUR OBSERVATIONS UNDERSTANDING THE CONTENTS OF CHAT LEAKATE THAT SHOW STRICT RELATIONSHIPS BETWEEN AKIRA AND BLACKBASTA OPERATORS [3] [4] LEADS US TO CONCLUDING THAT AKIRA IS USING THE BRUTED TOOL (HIGH CONFIDENCE). FROM THE FIRST ANALYSES ON SOME ITALIAN VICTIMS IMPACTED BY THE GROUP, NO DIRECT EVIDENCE OF BRUTEFORCING OR ALTERNATIVE METHODS FOR INITIAL ACCESS SUCH AS PHISHING OR EXPLOITATION OF VULNERABILITY ON DEVICES EXPOSED TO THE PUBLIC NETWORK EMERGED. WE HAVE EXPANDED OUR VIEW BY COMMUNICATING WITH OTHER ATTACKED COMPANIES WHO HAVE CONFIRMED THAT THEY HAVE EDGE DEVICES THAT FALL UNDER THE LIST OF THOSE TARGETED BY BRUTED. THE TOOL OFFERS OPERATORS AUTOMATION FROM BULK SCANNING THROUGH TO BRUTEFORCE STEPS WITH PROXY SOCKS5 ROTATION, CUSTOM USER-AGENTS BY DEVICE TYPE, SUBDOMAINS BRUTEFORCING AND SSL CERTIFICATE ANALYSIS TO CREATE TARGETED PASSWORD LISTS [5][6].

THE FOLLOWING TECHNOLOGIES ARE WITHIN THE SCOPE OF THE TOOL

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

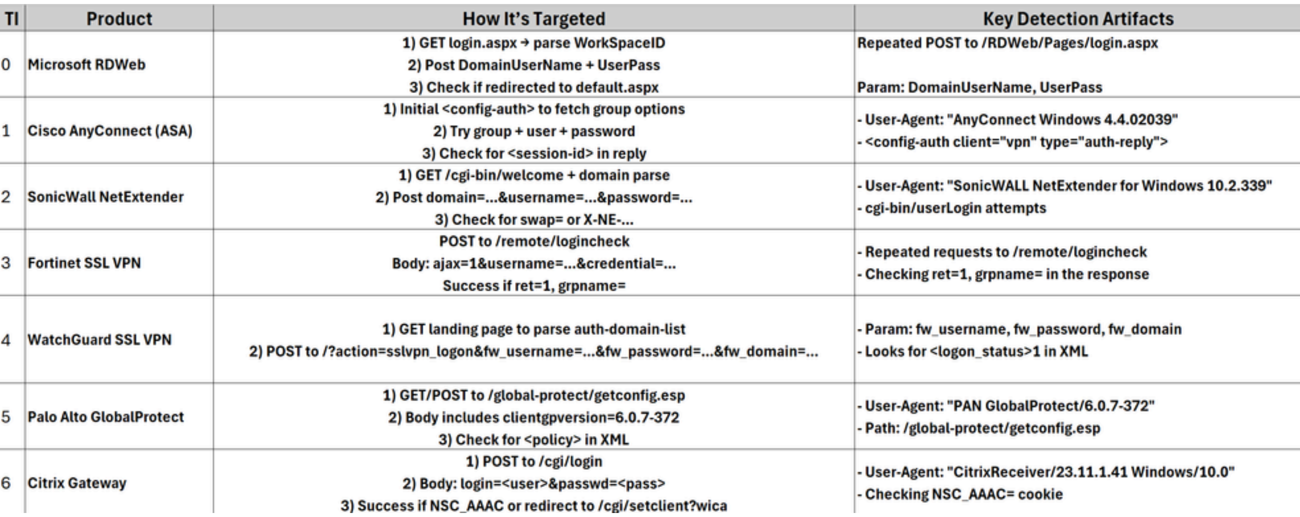
ONCE THE TOOL HAS FOUND THE CORRECT CREDENTIALS, IT SAVES THOSE CREDENTIALS IN A FILE WITH NOTIFICATION TO THE ATTACKER VIA TELEGRAM AND OTHER EXTERNAL API. SUBSEQUENTLY, OPERATORS MANUALLY USE THE OBTAINED CREDENTIALS TO ACCESS THE INFRASTRUCTURE BY GAINING INITIAL ACCESS FROM WHICH THEY THEN EXECUTE LATERAL MOVEMENT, INSTALL AND USE MALWARE IN PREPARATION FOR RANSOMWARE EXECUTION. SUPPORTING OUR THESIS WERE INERENT SSL VPNS LOGS OF ONE OF THE ITALIAN VICTIMS IMPACTED. ANALYSIS IN THE TWO DAYS PRIOR TO THE ATTACK LOGS WERE SUFFICIENT TO LEAD TO THOSE IP ADDRESSES :

- 141.98.80.134
- 141.98.80.144
- 45.227.255.84
- 46.161.27.99

IN PARTICULAR THE IP 46.161.27.99 BELONGS TO A SUBNET KNOWN SINCE NOVEMBER 2024 AND CITED BY SEVERAL AUTHORITATIVE SOURCES INCLUDING CISA IN A BULLETIN ABOUT BLACKBASTA [7], THE SUBSET BELONGS TO AS43350 [8] (NFORCE, NETHERLANDS). THE REUSE OF HOSTING USED BY BLACKBASTA IN AN AKIRA BRUTEFORCE OPERATION INCREASES THE LIKELIHOOD OF OPERATIONAL RELATIONSHIPS BETWEEN THE TWO RAAS. WE ADD THAT HYPOTHETICALLY, OPERATORS OF THE CACTUS RANSOMWARE COULD ALSO HAVE ACCESS TO THE TOOL. ALTHOUGH THERE IS NO PROOF ABOUT THE FACT THAT THIS GROUP ALSO HAD RELATIONSHIPS WITH BLACKBASTA MAY HAVE ACCESS TO THE BRUTED FRAMEWORK.

MITIGATIONS

BELOW WE REPROPOSE THE TABLE CREATED BY ECLECTICIQ AFTER THEY HAVE ANALYZED THE TOOL BY HAVING ACCESS TO PART OF THE FRAMEWORK SERVERS [9]. THESE VALUES ARE SPECIFIC TO DEVICE TYPES AND COULD BE CHANGED IN THE FUTURE BY ATTACKERS.

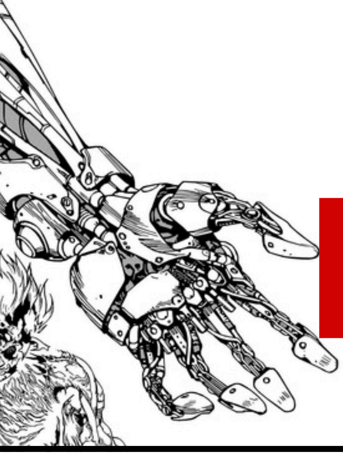


TI	Product	How It's Targeted	Key Detection Artifacts
0	Microsoft RDWeb	1) GET login.aspx → parse WorkSpaceID 2) Post DomainUserName + UserPass 3) Check if redirected to default.aspx	Repeated POST to /RDWeb/Pages/login.aspx Param: DomainUserName, UserPass
1	Cisco AnyConnect (ASA)	1) Initial <config-auth> 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=sslvpn_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 clientgpversion=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

N ADDITION TO THESE ARTIFACTS WE PROPOSE THE FOLLOWING TECHNIQUES FOR ROBUST AND EFFECTIVE POSTURE AS A RESPONSE TO BRUTED:

LOG POLICY

ROBUST AND EFFECTIVE LOG MANAGEMENT IS ONE OF THE PRIMARY WAYS TO BE ABLE TO USE DETECTION AND TRAFFIC ANALYSIS TOOLS EFFECTIVELY. LOG RETENTION MUST BE SUFFICIENT FOR POTENTIAL INVESTIGATIONS OR INCIDENT RESPONSE PROCESSES.



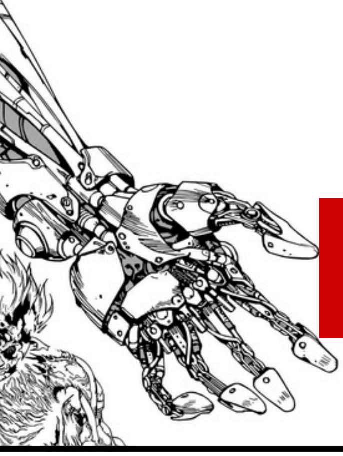
MITIGATIONS

MFA & PASSWORD/ACCESS POLICY

FOR ANY POINT OF ACCESS FROM A PUBLIC NETWORK [EG:/ VPN, RDPWEB] THEY NEED TO INTEGRATE MFA, PARTICULARLY IF THE DEVICES ARE ON THE TARGET LIST USED BY BRUTED. ATTACKERS SUCH AS AKIRA ARE CHARACTERIZED BY A HIGH DEGREE OF ADAPTABILITY, AND GIVEN THE FOCUS ON ITALIAN ORGANIZATIONS WE URGE IMPLEMENTING MFA ON ALL EDGE DEVICES PRESENT. WE ADVISE AGAINST THE USE OF MFA VIA SMS, WHICH COULD BE BYPASSED BY ATTACKS SUCH AS SIM SWAP. A CHECK ON ACCOUNT-LEVEL ACCESS ATTEMPTS ACCOMPANIED BY TIME CORRELATIONS [EG:/ ATTEMPT/ACCESS OUTSIDE OF BUSINESS HOURS] WITH PROFILE BLOCKING IN CASE OF POTENTIAL VIOLATION ARE EFFECTIVE TECHNIQUES TO MITIGATE THE ROTATION OF SOURCE ADDRESSES OF REQUESTS. THE USE OF HONEYPOT ACCOUNTS WITH [INTENTIONALLY] WEAK PASSWORDS CAN BE INTEGRATED AND MONITORED TO BE ABLE TO DETER ATTACKER EFFORTS BY BLOCKING SOURCE ADDRESSES OR REDIRECTING TO SANDBOX ENVIRONMENTS. FINALLY, A STRONG PASSWORD POLICY SHOULD BE THE BASIS FOR PREVENTION TO BRUTEFORCING OPERATIONS.

LEAST PRIVILEGE POLICY

ACCOUNTS FOR VPN/FIREWALL/RDP ACCESS SHOULD HAVE ONLY THE PRIVILEGES NECESSARY FOR THE FUNCTIONS REQUIRED BY THE USER REMOVING ACCESS OR ROLES THAT COULD BE ABUSED BY ATTACKERS TO MOVE ON TO THE NEXT STAGES OF THEIR ATTACKS.



MITIGATIONS

PATCH MANAGEMENT

PRIORITIZE PERIMETER DEVICES FOR PATCHING POTENTIAL EXISTING AND FUTURE VULNERABILITIES. SINCE THE BRUTED FRAMEWORK INCLUDES BULK SCANNING FEATURES OPERATORS COULD IMPLEMENT FILTERING FOR VULNERABILITIES THAT MAY BE ABUSED TO GAIN INITIAL ACCESS. KEEPING EXPOSED DEVICES UP-TO-DATE ALLOWS THEM TO PLAY AHEAD OF ATTACKERS WHO, LIKE AKIRA, FOCUS THEIR ATTENTIONS ON THE PERIMETER OF ORGANIZATIONS. REMOVE DEFAULT ACCOUNTS AND UNUSED SERVICES TO REDUCE THE ATTACK SURFACE.

RESPONSE PLAN

PREPARE EMPLOYEES AND NETWORK ADMINISTRATORS IN RESPONSE PROCESSES WHEN A BRUTEFORCING OR ILLICIT ACCESS ATTEMPT IS DETECTED. BETWEEN PROCESSES SHOULD BE CLARIFIED PASSWORD RESET METHODS, ADHERING TO THE PASSWORD POLICY, TO NULLIFY THE EFFORTS OF ATTACKERS AFTER THEY HAVE OBTAINED VALID CREDENTIALS.

IOC IDENTIFIED

141.98.80.134

141.98.80.144

45.227.255.84

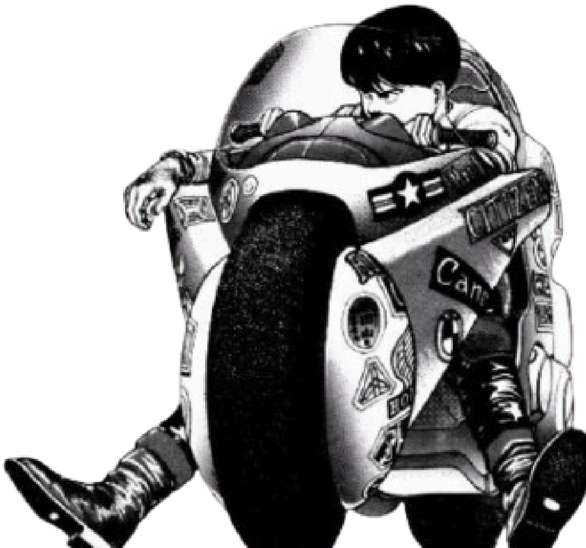
46.161.27.99

TOOLS

AKIRA IS PARTICULARLY QUICK TO REACH THE IMPACT PHASES BETWEEN EXFILTRATION OF FILES AND EXECUTION OF THEIR RANSOMWARE, WITH OPERATIONS COMPLETED IN LESS THAN 24 HOURS [10] FROM INITIAL ACCESS MAKES THE NEED FOR PERSISTENCE UNNECESSARY BY AVOIDING LEAVING TRACES ON THE AFFECTED NETWORKS. DESPITE THE SPEED AND STEALTH OF THE OPERATORS SEVERAL EXTERNAL ANALYSES HAVE BEEN ABLE TO IDENTIFY THE CURRENT STATE OF THE GROUP AND THE TOOLS, IN THIS SECTION WE WILL TRY TO COVER THE MAIN COMPONENTS OBSERVED

SHARPHOUND [11]

DATA COLLECTOR WRITTEN IN C# FOR BLOODHOUND [12], TOOL USED FOR VISUALIZING ACCESS/RELATIONS/CONFIGURATIONS IN ACTIVE DIRECTORY (AD) ENVIRONMENTS. THANKS TO THE USE OF LDAP AND SMB PROTOCOLS THE STATUS OF THE DIFFERENT AD COMPONENTS IS SAVED IN JSON FORMAT (COMPRESSED IN .ZIP) THE STATE OF THE DIFFERENT AD COMPONENTS SO THAT THEY CAN THEN BE VISUALIZED VIA GRAPHS SIMPLIFYING THE DISCOVERY OF USEFUL PATHS FOR OBTAINING ACCESS NEEDED FOR ATTACK OPERATIONS. AD NETWORKS CAN CONTAIN UNINTENDED PATHS THAT CAN MAKE UNWANTED PRIVILEGES ESPECIALLY ON COMPLEX ENVIRONMENTS WITH A MEDIUM/HIGH NUMBER OF OBJECTS (EG:/ COMPUTERS, USERS, GPO). THE BLOODHOUND FRAMEWORK AND RELATED DATA COLLECTORS ARE AVAILABLE FREE OF CHARGE AND WE ENCOURAGE ORGANIZATIONS TO USE THEM TO BENEFIT FROM THE KIND OF (SIMPLIFIED) INSIGHT OFFERED BY ALLOWING THEM TO GAIN A DEEPER UNDERSTANDING OF THE NETWORK AND ADDRESS POTENTIAL ABUSE POINTS.



IN ORDER TO DETECT THE USE OF SHARPHOUND IT IS ADVISABLE TO MONITOR THE FOLLOWING EVENT ID TRIGGERED BY THE TOOL, IMPORTANT TO FILTER ALERTS TO AVOID FALSE-POSITIVES THAT MIGHT CONFUSE SIEM OR OTHER MONITORING SOLUTIONS.

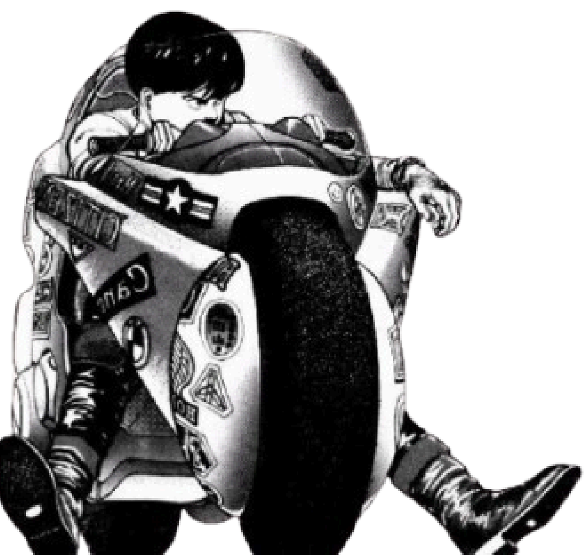
- 4648 - USE OF CREDENTIALS DIFFERENT FROM THE USER IN USE, SUCH AS RUNAS COMMAND CALLS

- 5145 - ACCESS TO NETWORK SHARING, THE DATA COLLECTOR EXECUTE (IF RQUESTED BY THE OPERATOR) A HIGH NUMBER OF SMB REQUESTS FOR INFORMATION COLLECTION.

- 4662 - TRIGGER ENABLED WHEN AN OPERATION IS PERFORMED ON A SPECIFIC OBJECT. SELECTING SPECIFIC COMPONENTS (INCLUDING CRITICAL COMPONENTS) AND ENABLING THE SACL (SYSTEM ACCESS CONTROL LIST) CAN DETECT ENUMERATION ATTEMPTS BY THREATS WITH INTERNAL ACCESS.

- 257/258 (SYSMON) - AMONG THE DATA COLLECTED BY THE COLLECTOR ARE THE NAMES OF THE INTERNAL WORKSTATIONS VIA DNS, AN UNUSUAL SPIKE IN THESE ANOMALOUSLY DISTRIBUTED QUERIES ARE A SIGNAL TO CONSIDER

- 3 (SYSMON) - SHARPHOUND MAKES CONNECTIONS TO PORTS 389/636 (LDAP/LDAPS) AND 445 (SMB) TO DOMAIN CONTROLLERS AND HOSTS IN THE SAME NETWORK SEGMENT CREATING A SIGNIFICANT VOLUME OF THESE CONNECTIONS IN A SHORT PERIOD OF TIME.

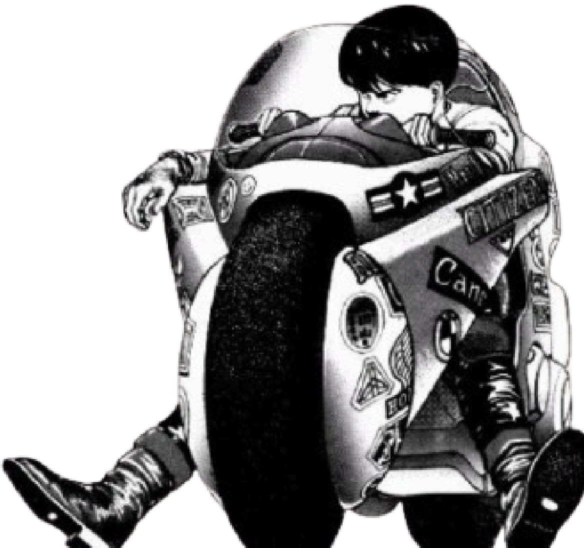


IN ADDITION TO WINDOWS EVENT IDS, LDAP QUERIES CAN BE MONITORED USING EVENT TRACING FOR WINDOWS (ETW) ADDING GRANULARITY AND ACCURACY. BLOODHOUND COLLECTORS USE THE "SAMACCOUNTTYPE=" FILTER EXTENSIVELY, FOR EXAMPLE, TO GET ALL USERS WITH (SAMACCOUNTTYPE=805306368) AND COMPUTERS WITH (SAMACCOUNTTYPE=805306369). STICKING WITH ETW YOU CAN TRACK CALLS TO APIS AS NETSESSIONENUM AND NETWKSTAUSERENUM USED IN THE ENUMERATION PHASE.

LASTLY, CREATING BAIT-OBJECTS VISIBLE ONLY THROUGH LDAP LENDS CONSIDERABLE SUPPORT WHICH, RELATED TO WHAT WAS EXPRESSED ABOVE, INSERTS AN HIGHER CONFIDENCE LEVEL FOR DETECTION AND RESPONSE TO SHARPHOUND.

USEFUL RESOURCES

- SNIFFING OUT SHARPHOUND ON ITS HUNT FOR DOMAIN ADMIN [13]
- SHARPHOUND DOCUMENTATION [14]
- BLOODHOUND COLLECTORS CHEATSHET [15]
- SHARPHOUND DETECTION [16]
- SACL IMPLEMENTATION [17]
- CONFIGURE ETW [18]

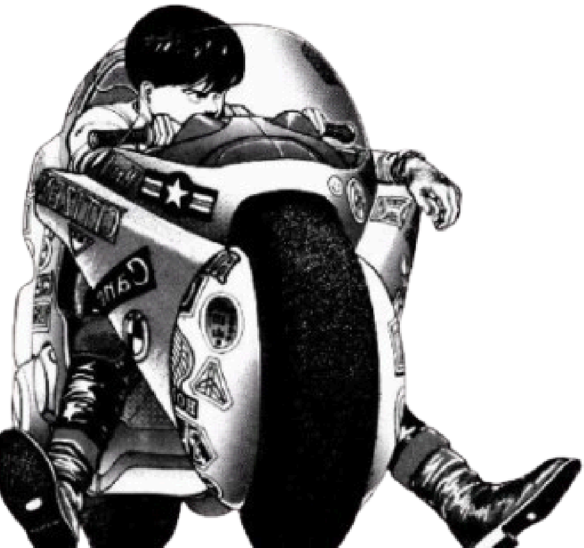


COMSVCS.DLL

"LIVING OFF THE LAND" (LOL) TECHNIQUES USE BINARIES OR DLL LIBRARIES PRESENT IN THE OPERATING SYSTEM AND THEREFORE CONSIDERED LEGITIMATE MORE THAN SIGNED BY MICROSOFT IN THE CASE OF WINDOWS OS. ABUSING INTERNAL COMPONENTS MAKES IT EASY TO EVADE TRADITIONAL ENDPOINT SECURITY SOLUTIONS. THERE ARE MULTIPLE TACTICS THAT CAN BE ACHIEVED BY DIFFERENT LOL BUT IN THE CASE OF AKIRA, PERSISTENT USE OF COMSVCS.DLL TO DUMP NTDS WAS NTDS.DIT, A FILE PRESENT IN DOMAIN CONTROLLERS CONTAINING THE HASHES OF AD NETWORK USERS, AND MEMORIA OF THE LSASS PROCESS CONTAINING CREDENTIALS OF (AUTHENTICATED) WORKSTATION LEVEL USERS. A COMMON USE OF THIS DLL IS TO RUN IT THROUGH AN EXECUTABLE LOL PRESENT ON WINDOWS IN ORDER TO PERFORM SPECIFIC FUNCTIONS WITHIN THE LIBRARY, RUNDLL32.

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

FIRST, ONE MUST HARDEN THE NETWORK AND INDIVIDUAL WORKSTATIONS TO PREVENT OBTAINING ADMINISTRATOR (NETWORK/LOCAL) ACCESS, WHICH REMAINS THE ONLY REQUIREMENT FOR INTERACTING WITH NTDS.DIT AND THE LSASS PROCESS. IN ADDITION MONITORING THE USE OF COMSVCS.DLL IN COMBINATION WITH RUNDLL32.EXE EVEN BY USERS WITH ADMINISTRATOR ACCESS IS AN EXCELLENT TRIGGER TO REVEAL MALICIOUS ACTIONS. THE EVENT ID 7 (IMAGE CREATION, SYSMON) ON THE DLL WITH SUCH A FILTER AND OTHER UNUSUAL PROCESSES SUPPORTS THIS DETECTION RULE.



VIEWING THE USE OF COMSVCS.DLL DOES NOT TURN OUT TO BE AN EFFECTIVE CHOICE GIVEN THE HIGH NUMBER OF FALSE POSITIVES THAT MIGHT EMERGE BEING A COMPONENT PRIMARILY USED AND MANAGED BY THE OPERATING SYSTEM AND LICIT PROGRAMS. TO COMPENSATE FOR THIS DISADVANTAGE ONE CAN FOCUS ON 2 SPECIFIC EVENT IDS:

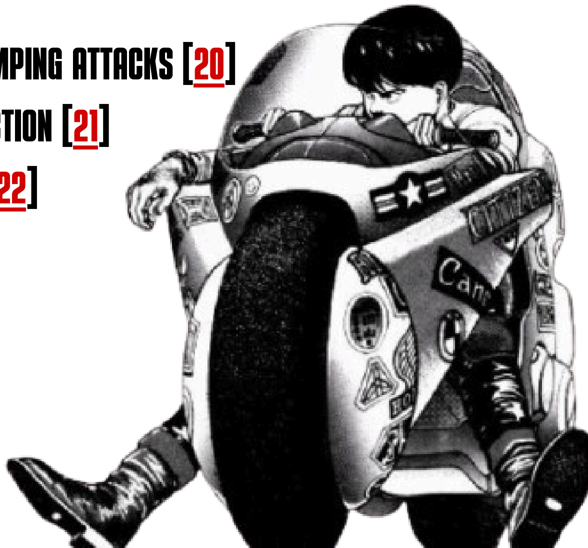
- 10 (SYSMON) = ACCESS ATTEMPT TO LSASS.EXE PROCESSES (ONLY WITH LOW VALUE PID) FROM NON-SYSTEM PROCESSES ARE A STRONG SIGNAL OF ABUSE MAKING A MONITORING IMPLEMENTATION ON THIS SPECIFIC EVENT ID SUFFICIENT.

- 4656 = THE TRIGGER FOR THIS EVENT ID IS THE OPENING OF A HANDLE ON AN OBJECT, SUCH AS NTDS.DIT FILE. ALONG WITH THIS YOU CAN ALSO INTEGRATE THE ID 4663 FOR ANY ACCESS TO THE ATTENDED FILE. LIKE LSASS.EXE ALSO NTDS.DIT SHOULD NOT BE SUBJECT TO INTERACTION FROM NON-SYSTEM USERS/PROCESSES.

SYSMON PLAYS AN INDISPENSABLE ROLE OFFERING A GRANULAR VIEW ON OPERATIONS CARRIED OUT IN WORKSTATIONS NECESSARY FOR THE EXECUTION OF LOL TECHNIQUES. GIVEN THE SENSITIVE NATURE OF THE FILE/PROCESS TARGETED BY ATTACKERS, SOAR SYSTEMS CAN DISABLE THE ACCOUNT WHICH ORIGINATED THE REQUEST IN ADDITION TO NOTIFYING NETWORK ADMINISTRATORS.

USEFUL RESOURCES

- 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]



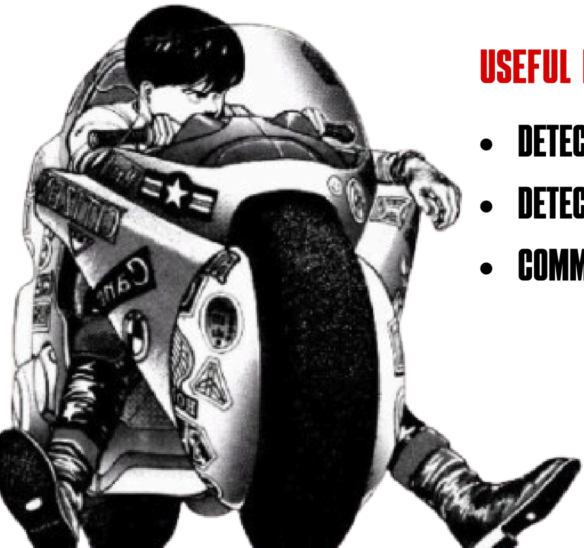
EXFILTRATION

THE TOOLS FILEZILLA, RCLONE AND WINSCP TOGETHER WITH WINRAR ARE THE MAIN VECTORS FOR DATA THEFT BY AKIRA IN THE PRE-ECRYPTION PHASES. CHOICE OF LEGITIMATE TOOLS ALLOW AVOIDANCE OF DETECTION BY ANTI-VIRUS AND EDR MAKING PREVENTION POSSIBLE ONLY WITH SPECIFIC CONTROLS ON THESE TOOLS. PROTECTION FROM EXFILTRATION TACTICS PROTECTS ORGANIZATIONS FROM ADDITIONAL PRESSURE IN NEGOTIATION BY AKIRA OR OTHER RAAS IMPLEMENTING DOUBLE EXTORTION IN THEIR OPERATIONS.

- APPLOCKER IS A DIRECT AND EFFECTIVE SOLUTION TO RESTRICT THE USE OF LEGITIMATE APPLICATIONS THAT ARE NOT CONSIDERED NECESSARY BY THE ORGANIZATION. VIA WHITELISTING IT RESTRICTS THE EXECUTION OF EXECUTABLES SUCH AS THOSE MENTIONED ABOVE BUT ALSO FOR RDP PROGRAMS EXTENSIVELY USED BY RANSOMWARE ATTACKERS.

- DLP (DATA LOSS PROTECTION) SOLUTIONS TO BLOCK THEFT ATTEMPTS BASED ON CONTENT OR EXECUTION CONTEXT. DESTINATIONS TO CLOUD SERVICES SUCH AS GOOGLE, MEGA AND SIMILARS CAN BE DETECTED OR/AND BLOCKED.

- MONITORING OF OUTBOUND TRAFFIC SHOULD BE A COMMON PRACTICE WITH A BALANCE BETWEEN AUTOMATED AND MANUAL ANALYSIS TO BE ABLE TO IDENTIFY THE SOURCE OF THEFT AND TRIGGER CONTAINMENT PROCESSES



USEFUL RESOURCES

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

BYOVD

BRING-YOUR-OWN-DRIVER (BYOVD) IS A TECHNIQUE THAT EXPLOITS THE DIGITAL FREQUENCES OF VULNERABLE DRIVERS THAT MAY LEAD TO PRIVILEGE ESCALATION, BLOCKING OF PROTECTED PROCESSES OR OTHER POSSIBLE RESIDENT KERNEL OPERATIONS CONTEXT IN WHICH THE DRIVER IS LOCALIZED ONCE INSERTED INTO THE SYSTEM. AKIRA HAD BEEN OBSERVED USING A MODIFIED VERSION OF TERMINATOR [27] IN 2024 AND 2025 THAT USES A VULNERABLE VERSION OF ZAMGUARD64.SYS (ZEMANA ANTI-MALWARE) [28]. THE TOOL SUCCEEDS IN STOPPING PROTECTED PROCESSES OF SYSTEMS SUCH AS AV, EDR AND OTHER SECURITY SOLUTIONS. ONCE THE DRIVER IS INSTALLED IT BECOMES DIFFICULT TO IDENTIFY MALICIOUS ACTIONS WITH TRADITIONAL SOLUTIONS SINCE KERNEL-LEVEL ACTIONS ARE CONSIDERED TRUSTED BY DEFAULT, THE MAIN MITIGATION METHODS WE PROPOSE ARE :

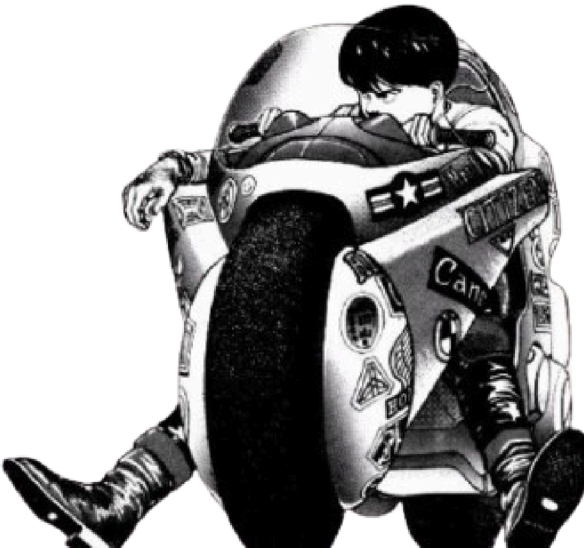
- WHITELISTING OF DRIVERS INSTALLED VIA WDAC (WINDOWS DEFENDER APPLICATION CONTROL) KEEPING ONLY STRICTLY NECESSARY DRIVERS VALID AND AVOIDING INSTALLATION OF THOSE NOT ON THE LIST, EVEN IF SIGNED.

- UPDATE ALL INSTALLED DRIVERS (ESPECIALLY ANTI-VIRUS AND EDR DRIVERS) TO PREVENT ABUSE OF INSTALLED DRIVERS THAT MAY CONTAIN VULNERABILITIES ABUSABLE BY ATTACKERS.

- MONITORING EVENT ID 6 (DRIVER LOADED, SYSMON) COMBINED WITH CORRELATION OF UNUSUAL PATH OR UNKNOWN HASH.

USEFUL RESOURCES

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



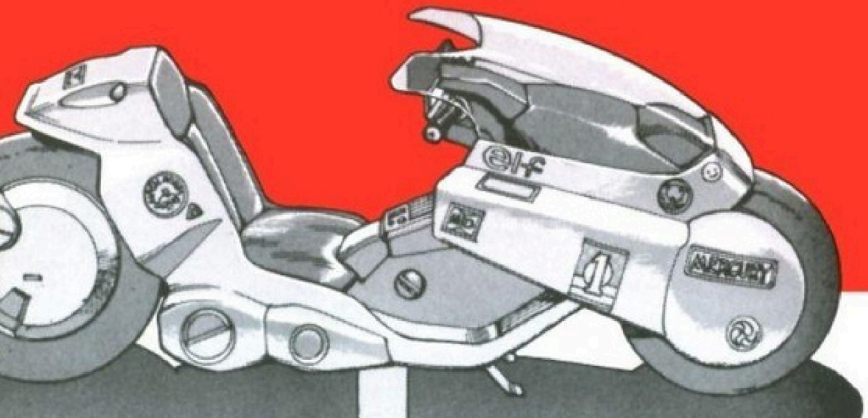
MISC

THE TOOLS COVERED IN THE PREVIOUS SECTION SHOULD NOT BE CONSIDERED A COMPLETE LIST, AND WE SUGGEST STAYING ABREAST OF THE GROUP'S MOVEMENTS IN THE FUTURE IN ORDER TO ADAPT BY MAINTAINING A PROACTIVE APPROACH TO PROTECTING ORGANIZATIONAL ASSETS. BELOW WE WOULD LIKE TO LAY OUT ADDITIONAL GUIDELINES THAT YOU CAN AFFIX TO YOUR NETWORKS TO REDUCE THE IMPACT FROM RANSOMWARE THREATS THAT, ACCORDING TO OUR ANALYSIS, CONTINUE TO INCREASE WITHIN THE BORDERS OF THE BEAUTIFUL COUNTRY.

1

PRIVILEGES MANAGEMENT

ACTIVE DIRECTORY NETWORKS SHOULD BE REVIEWED AND MODIFIED FOLLOWING THE TIERED ADMINISTRATION MODEL [30][31] TO ACHIEVE A SIMPLIFIED VISION AND MANAGEMENT OF INTERNAL SECURITY. IMPLEMENTATION OF JUST-IN-TIME POLICY [32][33] ALLOW PRIVILEGES TO BE OBTAINED, WHEN NEEDED, ONLY FOR AS LONG AS NECESSARY, AVOIDING LEAVING EXPOSED HIGH-INTEGRITY SESSIONS THAT CAN BE ABUSED BY ACTORS WITH INSIDE ACCESS



BACKUP MANAGEMENT

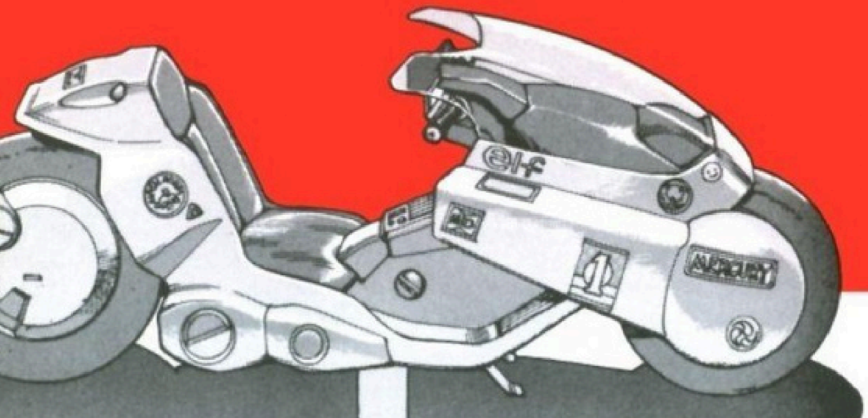
2

THE DAMAGE OF RANSOMWARE IS THE COMPROMISE OF DATA THAT OFTEN RESULTS IN A HALT TO THE ACTIVITIES OF THE IMPACTED COMPANY. FOLLOWING THE 3-2-1 RULE (3 COPIES ON 2 DIFFERENT MEDIA INCLUDING 1 OFF-SITE) FOR DATA MUST BE THE BASIS FOR BEING ABLE TO RESTORE ACTIVITIES. ATTACKERS HAVE ADAPTED AND OFTEN SEEK OUT SUCH BACKUPS TO DESTROY THEM, BACKUPS MUST BE PROTECTED THROUGH LOGICAL AIR GAPS, IMMUTABILITY AND OTHER METHODS.

3

ESXi HARDENING

INVESTIGATIONS HAVE CONFIRMED HOW AKIRA TAKES AIMS AT ESXi SYSTEMS IN ITS OPERATIONS. EFFECTIVE VLAN SEGMENTATION ASSOCIATED WITH JUMPBOX TO LIMIT DIRECT ACCESS AND/OR THE USE OF LOCKDOWN MODE FOR EXCLUSIVE ACCESS THROUGH VCENTER SPHERE ARE SIMPLE ACCORGEMENTS THAT MITIGATE COMPROMISE OF THIS TYPE OF ASSET. LOG AND BACKUP POLICIES MUST INLUDE ESXi FOR MONITORING PROCESSES.



4

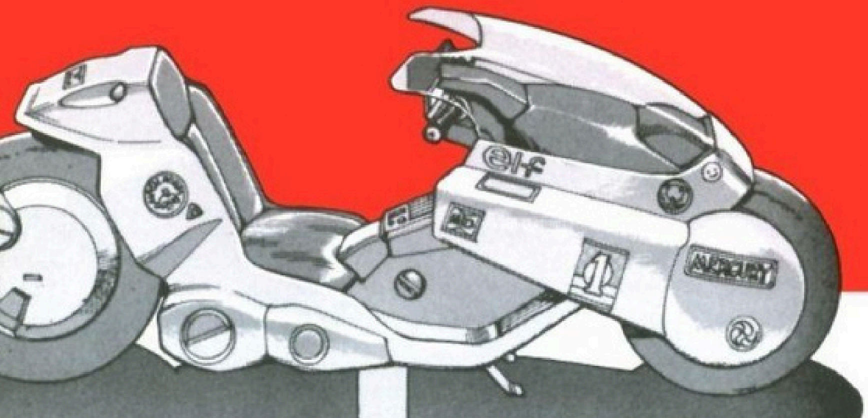
RECOVERY AND RESTORATION PROCESSES

TO KEEP THE PREPAREDNESS OF THE TEAM RESPONSIBLE IN RESPONDING TO ATTACKS SUCH AS RANSOMWARE HIGH, SIMULATIONS CAN BE RUN TO ASSESS THEIR EFFECTIVENESS AND EXECUTION TIME. IT IS NOT ENOUGH TO SIMPLY PREPARE PURELY THEORETICAL GUIDELINES, BUT THROUGH TESTING OF THESE GUIDELINES THEY CAN BE REEVALUATED AND ADAPTED TO THE ENVIRONMENT.

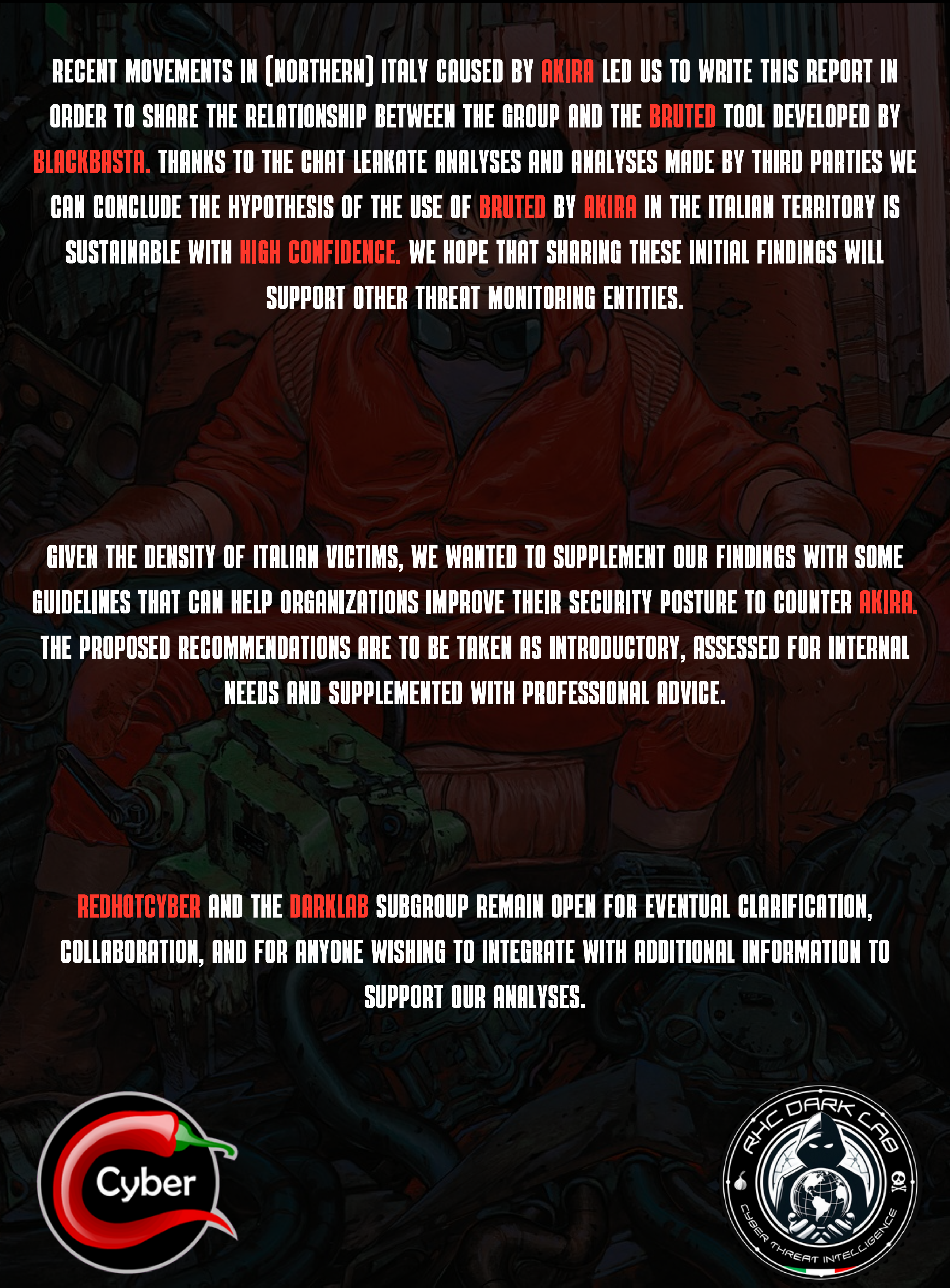
5

RISK EVALUATION

THERE IS OFTEN A TENDENCY TO THINK THAT RANSOMWARE ATTACKS ARE A THREAT TO LARGE COMPANIES OR SPECIFIC SECTORS SUCH AS GOVERNMENT. IN REALITY, MOST RANSOMWARE ATTACKS TEND TO FOCUS ON MEDIUM/SMALL BUSINESSES IN ADDITION TO LARGE ONES, ORGANIZATIONS NEED TO CONSIDER AND EVALUATE THEIR SECURITY INVESTMENT BY LOOKING FOR SOLUTIONS THAT FIT THEIR ENVIRONMENT AND BUDGET.



CONCLUSIONS



RECENT MOVEMENTS IN (NORTHERN) ITALY CAUSED BY AKIRA LED US TO WRITE THIS REPORT IN ORDER TO SHARE THE RELATIONSHIP BETWEEN THE GROUP AND THE BRUTED TOOL DEVELOPED BY BLACKBASTA. THANKS TO THE CHAT LEAKATE ANALYSES AND ANALYSES MADE BY THIRD PARTIES WE CAN CONCLUDE THE HYPOTHESIS OF THE USE OF BRUTED BY AKIRA IN THE ITALIAN TERRITORY IS SUSTAINABLE WITH HIGH CONFIDENCE. WE HOPE THAT SHARING THESE INITIAL FINDINGS WILL SUPPORT OTHER THREAT MONITORING ENTITIES.

GIVEN THE DENSITY OF ITALIAN VICTIMS, WE WANTED TO SUPPLEMENT OUR FINDINGS WITH SOME GUIDELINES THAT CAN HELP ORGANIZATIONS IMPROVE THEIR SECURITY POSTURE TO COUNTER AKIRA. THE PROPOSED RECOMMENDATIONS ARE TO BE TAKEN AS INTRODUCTORY, ASSESSED FOR INTERNAL NEEDS AND SUPPLEMENTED WITH PROFESSIONAL ADVICE.

REDHOTCYBER AND THE DARKLAB SUBGROUP REMAIN OPEN FOR EVENTUAL CLARIFICATION, COLLABORATION, AND FOR ANYONE WISHING TO INTEGRATE WITH ADDITIONAL INFORMATION TO SUPPORT OUR ANALYSES.