Lab 5.1: Developing an Adversary Emulation Plan

Introduction

Through this course, we've discussed the what, why, and how of Adversary Emulation. We've looked at executing existing emulation plans, implementing emulated TTPs to support those plans, and the processes around performing an Adversary Emulation engagement.

In this lab, we're going to take a step back and focus on creating our own emulation plan. The guidance and experience from this lab will help you create tailored Adversary Emulation plans to effectively improve the cyber defenses of your organization.

Objectives:

1. Develop a post-compromise emulation plan for a threat actor relevant to your organization
2. Extra credit: Execute your emulation plan on appropriate test infrastructure

Estimated Completion Time:

- Up to several hours, depending on the depth and comprehensiveness of your plan.

Requirements

1. Internet access – All we will need is the ability to research threat actors.

Overview

In Lab 1.2, we followed the CTID Adversary Emulation Library's FIN6 plan, executing it on the lab infrastructure. We were fortunate that an emulation plan already existed for FIN6. Numerous adversary emulation plans exist for other threat actors as well, both created by CTID and the community at large. However, we may find that a comprehensive emulation does not exist for a particular threat actor that we are interested in. In such a case, we'll need to use CTI to develop our own emulation plan.

In this lab, we'll discuss how to select a threat actor relevant to your organization, examine CTI to extract techniques, and compile those techniques into a usable plan.

Walkthrough

The first step in creating an Adversary Emulation plan is deciding which threat actor you'll be emulating. There are three primary concerns with selecting a good threat actor:

1. Do they target your industry?
2. Do they target your geographical location?
3. Is there sufficient CTI available?

For the purpose of this guide, we'll be further splitting this step into three parts based on the above concerns.

Step 1: Find Threat Actors Targeting Your Industry

As part of this walkthrough, we'll pretend to be performing this process for a Biotech firm. You can follow along with the walkthrough as is, or use this process as a guide for your own organization.

To find threat actors relevant to your organization, we navigate to the MITRE ATT&CK Groups page, found here:

https://attack.mitre.org/groups/

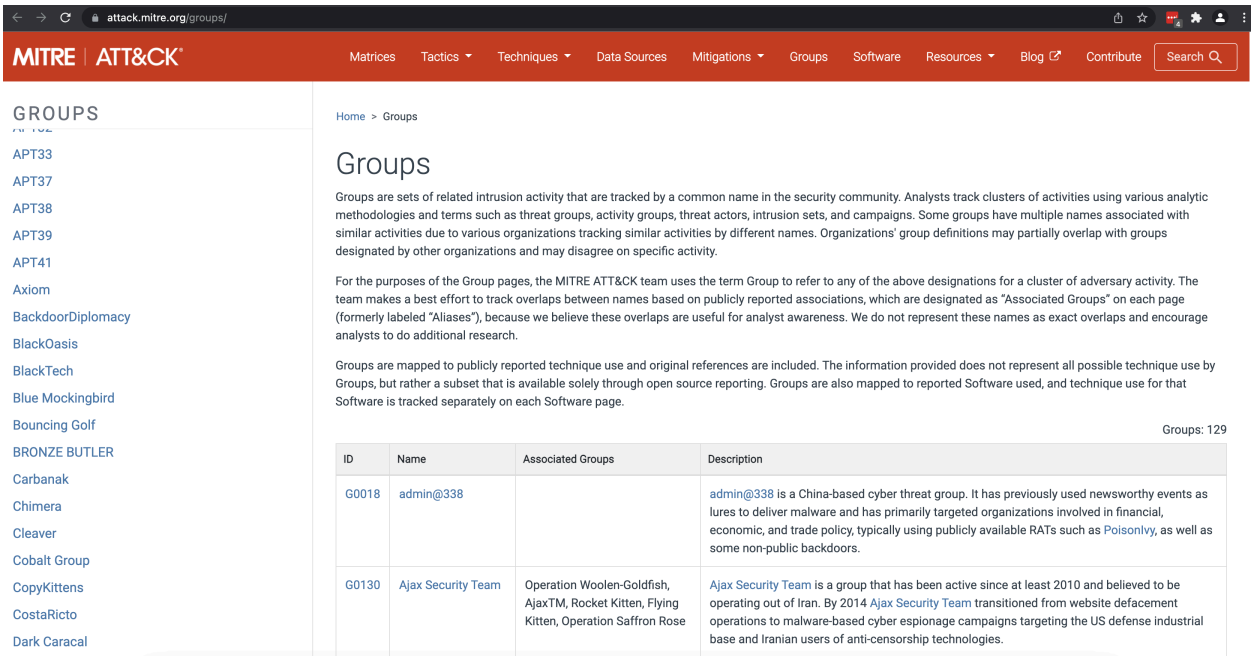


Figure 1. MITRE ATT&CK Groups page

On this page, we can see a listing of many threat actors with brief descriptions related to their behaviors and targets, which is exactly what we need. We'll search for our industry on this page, using the term "bio" to see broader results.

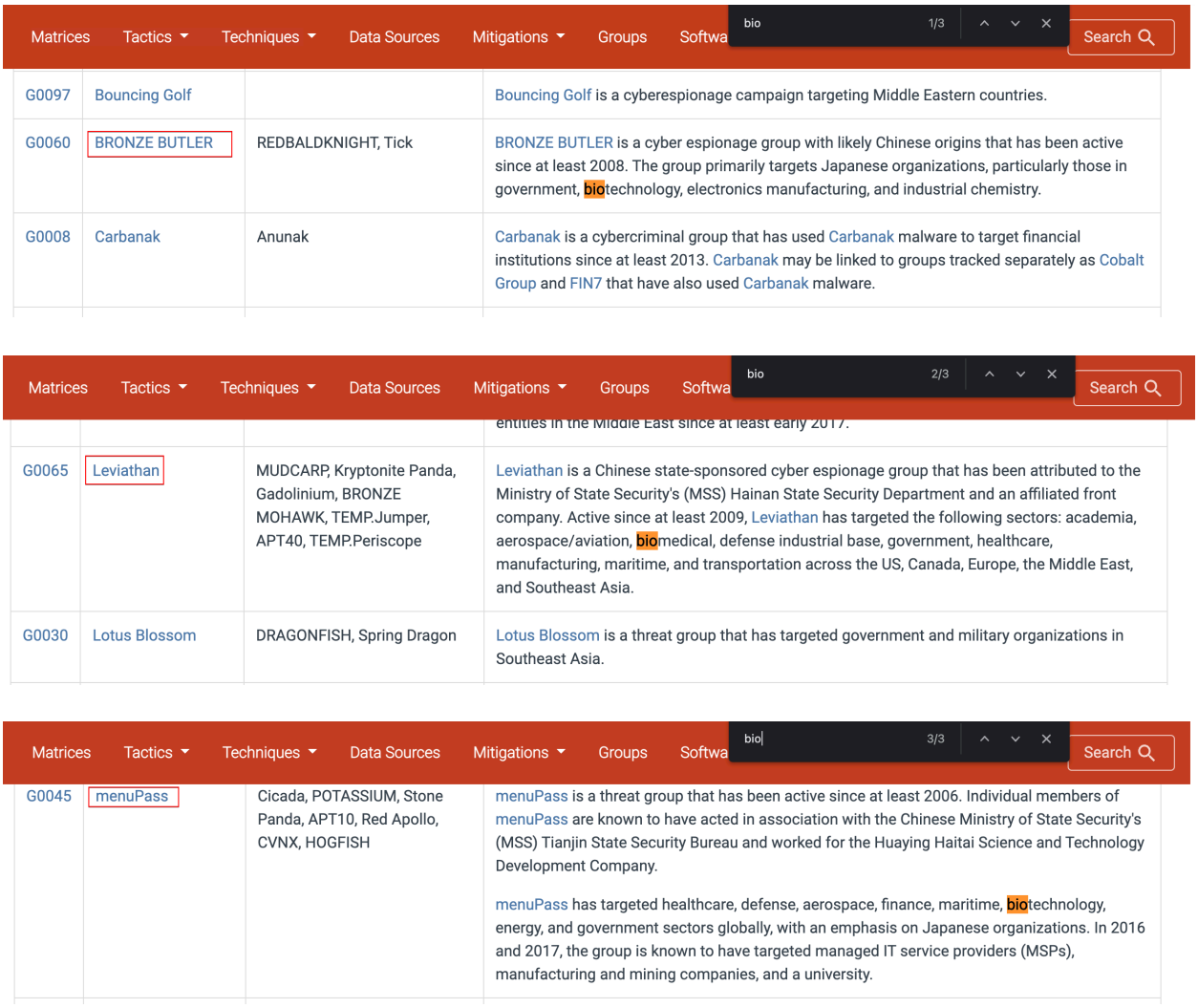


Figure 2. Threat Actors Targeting Biotech/Biomedical Firms

We see that three groups closely match our industry: Bronze Butler, Leviathan, and menuPass. Leviathan's description states that they have targeted the Biomedical industry in the past, but that is close enough to our industry to keep them in consideration.

Note: when performing this for your industry, consider searching using related terminology as well to expand your results. For example, an organization in the aviation industry may also be interested in threat actors targeting aerospace institutions.

Step 2: Trim Threat Actors by Geographic Targeting

Now that we have a list of threat actors that target our industry, let's check to see which ones have targeted our geographical region. We see that Bronze Butler primarily targets Japanese

organizations. Leviathan is known to have targeted North America, Europe, the Middle East, and Southeast Asia. Finally, menuPass has targeted organizations around the globe, with a greater focus on Japanese organizations. Assuming that we're a North American organization, we can trim the relevant threat actors list to Leviathan and menuPass.

Step 3: Select Threat Actor

With our trimmed list of threat actors that may be interested in targeting our organization, we can now select the one that will best serve our needs. The most important criteria we're concerned with is how much CTI is available. For this walkthrough, we are assuming that we do not have access to private CTI, and so will look only at what is publicly available.

Note: Your organization may have closed-source CTI from prior attacks. If that CTI is available to you and there is sufficient detail, that threat actor would likely be the most valuable one to emulate for your organization.

We examine the available CTI by accessing the specific group's ATT&CK page:

- Leviathan – https://attack.mitre.org/groups/G0065/
- menuPass – https://attack.mitre.org/groups/G0045/

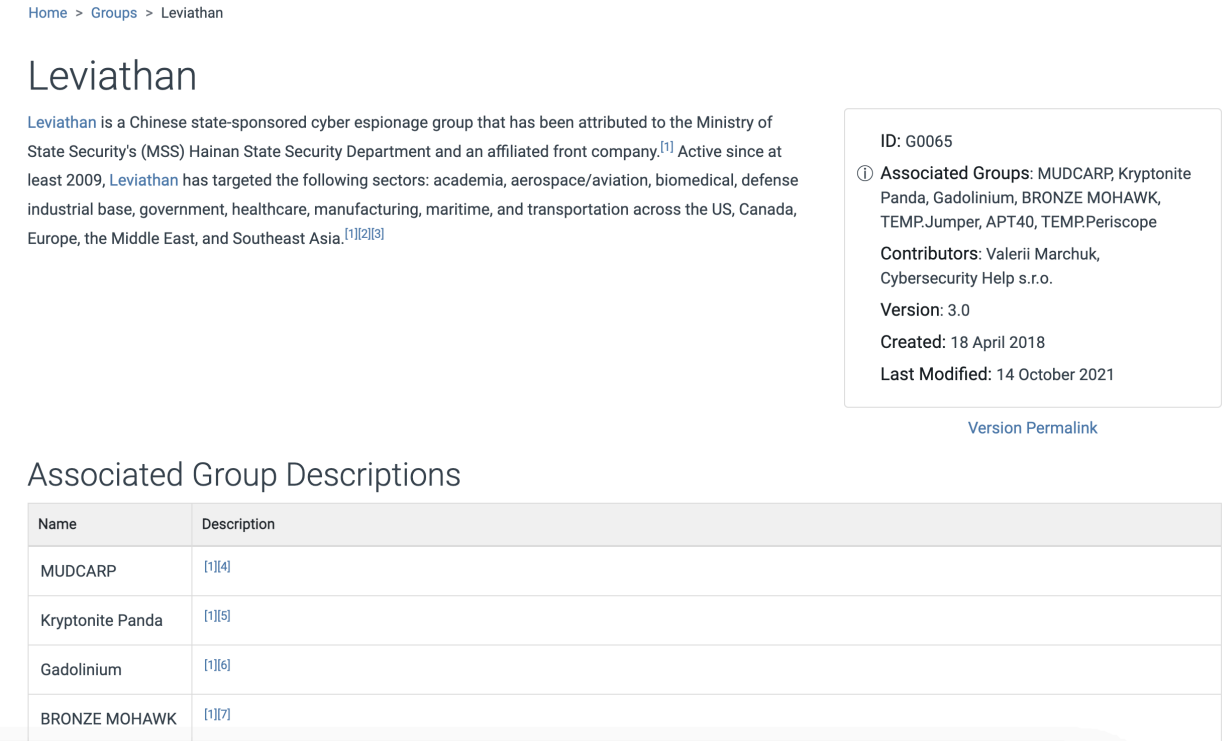


Figure 3. Leviathan ATT&CK Page

Home > Groups > menuPass

menuPass

menuPass is a threat group that has been active since at least 2006. Individual members of menuPass are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.[1][2]

menuPass has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.[3][4][5][6][7][1][2]

ID: G0045

Associated Groups: Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH

Contributors: Edward Millington; Michael Cox

Version: 2.1

Created: 31 May 2017

Last Modified: 11 October 2021

Version Permalink

Associated Group Descriptions

Name	Description
Cicada	[8]
POTASSIUM	[1][2]
Stone Panda	[3][9][1][2][8]
APT10	[3][9][10][1][8]

Figure 4. menuPass ATT&CK Page

Both Leviathan and menuPass have a fair amount of available CTI. There are many techniques listed for each group, along with associated software. In such an instance, selecting a threat actor could be done either based of any other criteria relevant to your organization, arbitrarily, or both could be emulated. For this lab we'll select menuPass, simply because there are more available references on their ATT&CK page.

References

1. CISA. (2021, July 19). (AA21-200A) Joint Cybersecurity Advisory – Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department.. Retrieved August 12, 2021.
2. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.
3. FireEye. (2018, March 16). Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries. Retrieved April 11, 2018.
4. Accenture iDefense Unit. (2019, March 5). Mudcarp's Focus on Submarine Technologies. Retrieved August 24, 2021.
5. Adam Kozy. (2018, August 30). Two Birds, One Stone Panda. Retrieved August 24, 2021.
6. Ben Koehl, Joe Hannon. (2020, September 24). Microsoft Security - Detecting Empires in the Cloud. Retrieved August 24, 2021.
7. SecureWorks. (n.d.). Threat Profile - BRONZE MOHAWK. Retrieved August 24, 2021.
8. Plan, F., et al. (2019, March 4). APT40: Examining a China-Nexus Espionage Actor. Retrieved March 18, 2019.

Figure 5. Leviathan References List

References

1. United States District Court Southern District of New York (USDC SDNY) . (2018, December 17). United States of America v. Zhu Hua and Zhang Shilong. Retrieved April 17, 2019.
2. US District Court Southern District of New York. (2018, December 17). United States v. Zhu Hua Indictment. Retrieved December 17, 2020.
3. Miller-Osborn, J. and Grunzweig, J.. (2017, February 16). menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations. Retrieved March 1, 2017.
4. Crowdstrike. (2013, October 16). CrowdCasts Monthly: You Have an Adversary Problem. Retrieved March 1, 2017.
5. FireEye. (2014). POISON IVY: Assessing Damage and Extracting Intelligence. Retrieved November 12, 2014.
6. PwC and BAE Systems. (2017, April). Operation Cloud Hopper. Retrieved April 5, 2017.
7. FireEye iSIGHT Intelligence. (2017, April 6). APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat. Retrieved June 29, 2017.
8. Symantec. (2020, November 17). Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign. Retrieved December 17, 2020.
9. Accenture Security. (2018, April 23). Hogfish Redleaves Campaign. Retrieved July 2, 2018.
10. Matsuda, A., Muhammad I. (2018, September 13). APT10 Targeting Japanese Corporations Using Updated TTPs. Retrieved September 17, 2018.
11. PwC and BAE Systems. (2017, April). Operation Cloud Hopper: Technical Annex. Retrieved April 13, 2017.
12. Twi1ight. (2015, July 11). AD-Pentest-Script - wmiexec.vbs. Retrieved June 29, 2017.
13. GREAT. (2021, March 30). APT10: sophisticated multi-layered loader Ecipekac discovered in A41APT campaign. Retrieved June 17, 2021.

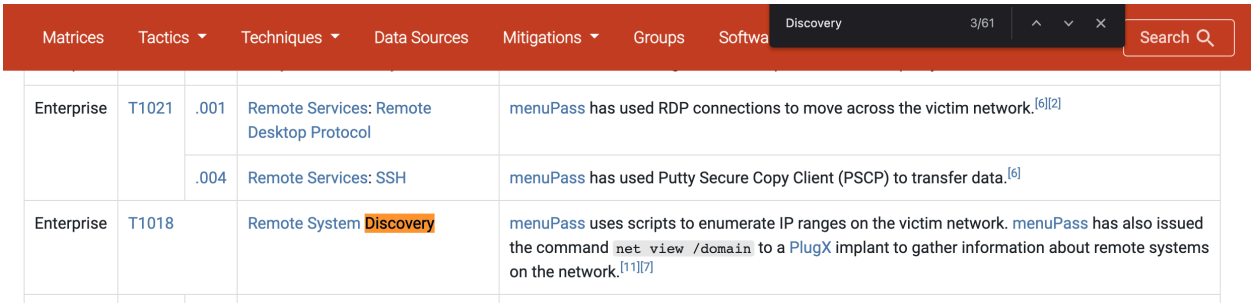
Figure 6. menuPass References List

Step 4: Select Techniques to Emulate

With our threat actor selected, we now need to figure out what techniques to select for our emulation plan. For this lab, we'll be finding only 3 techniques, focusing on post-compromise tactics. However, in general an emulation plan should include most, if not all, of the post-compromise tactics. Including initial access techniques can also add value to the emulation.

In searching for our three techniques, we'll look at the following tactics: Discovery, Credential Access, and Exfiltration, all of which are characteristic of most adversary campaigns.

Let's start with Discovery. Searching for the word "discovery" on the page, we can find the Remote System Discovery technique shown below.



Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	menuPass has used RDP connections to move across the victim network.[6][2]
		.004	Remote Services: SSH	menuPass has used Putty Secure Copy Client (PSCP) to transfer data.[6]
Enterprise	T1018		Remote System Discovery	menuPass uses scripts to enumerate IP ranges on the victim network. menuPass has also issued the command `net view /domain` to a PlugX implant to gather information about remote systems on the network.[11][7]

Figure 7. menuPass Remote System Discovery

Fortunately for us, the technique description includes the specific procedure that menuPass used to perform this discovery. We can add this to our list of techniques to emulate.

Note: We recommend capturing the technique and procedure along with the source it was retrieved from for future reference. Additional useful information can be captured in a notes

section as well. Finally, alternative procedures for the same technique can be researched and included. This can be beneficial in case the original technique fails to work for any reason.

The next tactic is Credential Access. Searching for “credential” on the page, we find three related techniques.

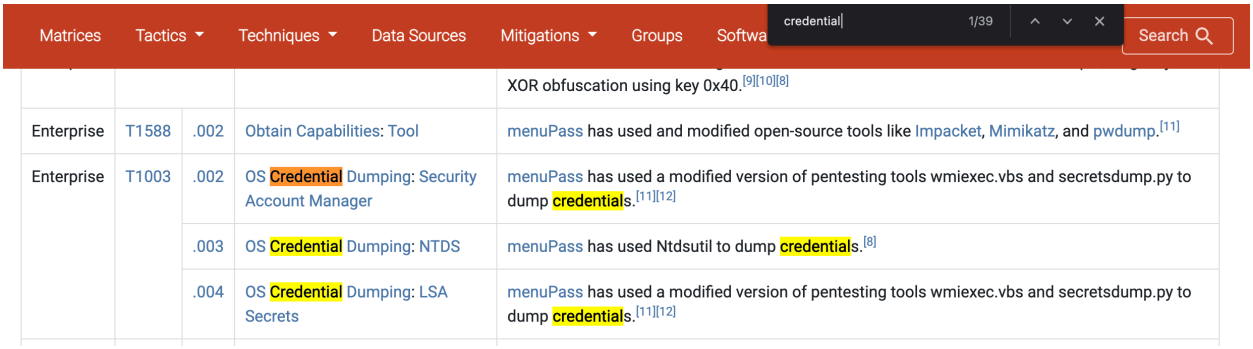


Figure 8. menuPass Credential Access

We’ll look at the first technique, OS Credential Dumping: Security Account Manager. The description tells us that “menuPass has used a modified version of wmiexec.vbs and secretsdump.py to dump credentials.” While this is good information, it doesn’t give us the specific procedure that menuPass used. We’ll need to dig in a little deeper by looking at the linked references. Let’s follow the link labeled as 11 to access one part of a larger report by PWC called “Operation Cloud Hopper Technical Annex”.

Searching for “secretsdump” takes us to the following information:

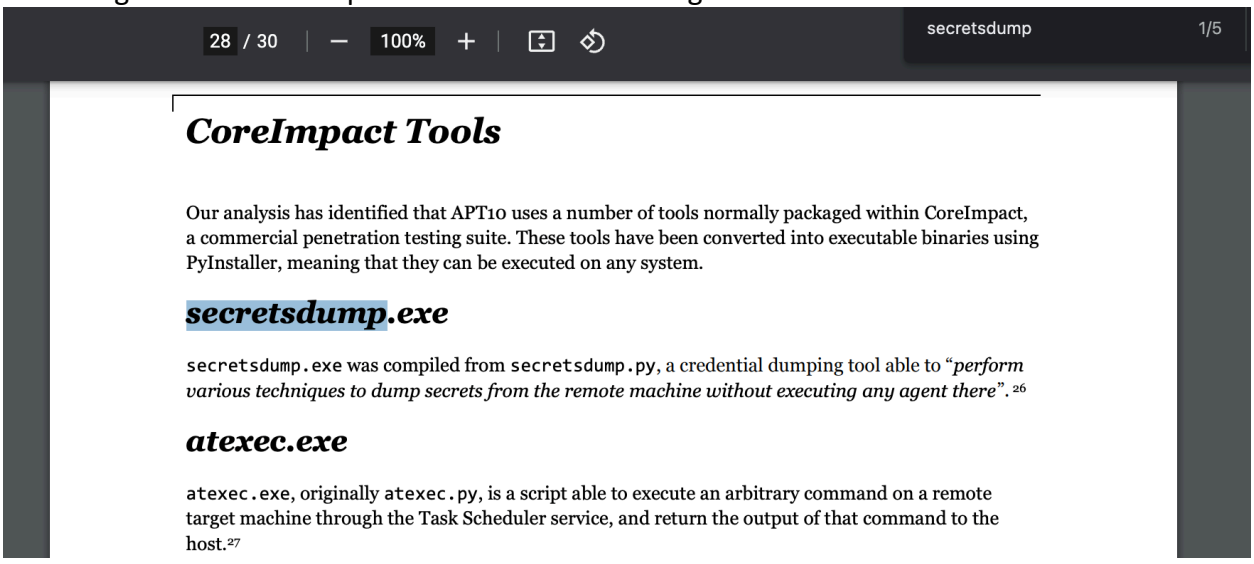


Figure 9. secretsdump.exe - PWC Report

This tells us that menuPass compiled Impacket’s secretsdump.py script to an executable before using it to dump credentials on target systems. Let’s add this to our list.

Finally, we take a look at exfiltration. Searching for exfiltration on the menuPass ATT&CK page returns only results related to collection. While the ATT&CK framework is a hugely valuable resource of adversary behaviors and is constantly being augmented, it unfortunately does not contain every single reported behavior. We'll need to look elsewhere for this missing information. Searching for "exfil" in the PWC report we just examined, we do find a result.

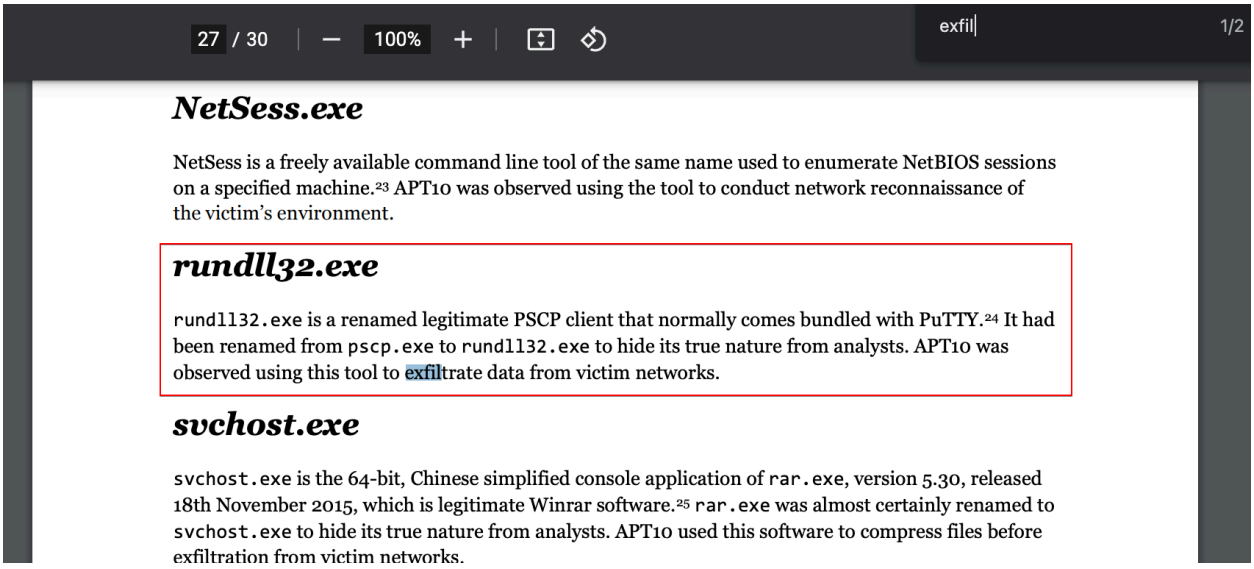


Figure 10. rundll32.exe – PWC report

We see that menuPass has been found to exfiltrate data from victims using PuTTY's pscp.exe, renamed to rundll32.exe. We'll take a note of this as well.

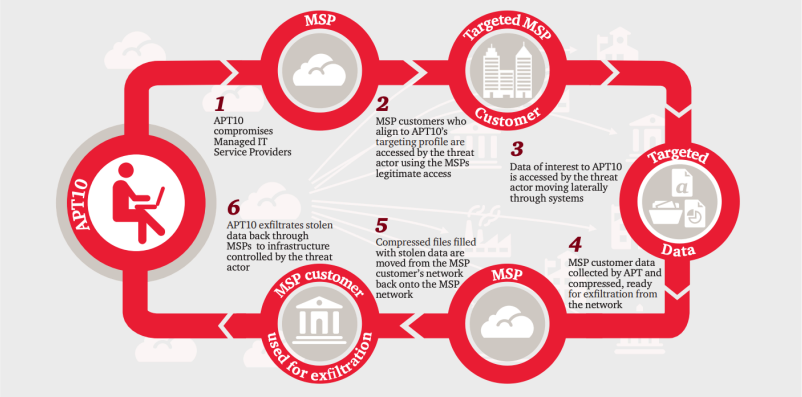
Again, for this lab, we're only going through gathering three techniques. To create a full emulation plan, you'll need to gather several techniques spanning the various adversary tactics.

Step 5: Determine the Attack Chain

While adversaries often follow a similar path of attack, there can be significant differences that set them apart from each other. To emulate the adversary as closely as possible, we should try to determine the path of attack our chosen threat actor has been found to follow. Fortunately for us, there are often sources that report on the attack path. Sometimes, these are presented as clean visuals. At other times, we'll need to dig through text to pull this information out.

Let's look at the main PWC report for this information. Scrolling down the report, we come across the following methodology section:

Shining a light on APT10's methodology



This section details changes made to APT10 tools, techniques and procedures (TTPs) post-2014, following its shift from Poison Ivy to PlugX. These TTPs have been identified as part of our incident response and threat intelligence investigations and have been used in both of the recent campaigns we have encountered. The examples provided in this section will be drawn from both of those campaigns.

Reconnaissance and targeting

It is often difficult to identify the early stages of a threat actor's preparation for an attack as these initial activities tend

Figure 14: Decoy document used by APT10 to target the Japanese education sector

Figure 11. PWC Report Methodology Section

Under the methodology section, we see text describing menuPass' behavior starting from initial compromise through exfiltration.

As part of the same campaign, we have also observed an email sent by APT10,[13] referencing a Scientific Research Grant Program, and targeting various Japanese education institutes including Meiji University[14] and Chuo University.[15] The email included a zip file containing a link to download a payload from one of APT10's servers, the ChChes Powersploit exploit, detailed in Annex B.

Initial compromise and lateral movement

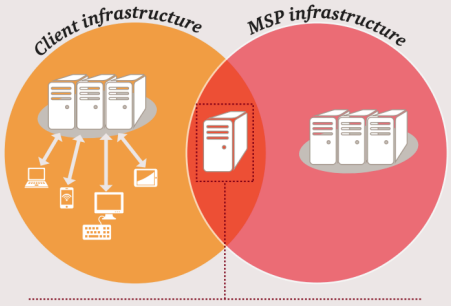
Once on a target network, the actor rapidly deploys malware to establish a foothold, which may include one or more systems that provide sustained access to a victim's network. As APT10 works to gain further privileges and access, it also conducts internal reconnaissance, mapping out the network using common Windows tools, and in later stages of the compromise using open source pentesting tools, detailed in Annex B.

This reconnaissance is run in parallel with the actor ensuring that it has access to legitimate credentials. We have observed that in cases where APT10 has infiltrated a target via an MSP, it continues to use the MSPs credentials. In order to gain any further credentials, APT10 will usually deploy credential theft tools such as mimikatz or PwDump, sometimes using DLL load order hijacking, to use against a domain controller, explained further in Annex B. Regular communications checks are then executed in order to maintain this level of access. In most cases, these stolen MSP credentials have provided administrator or domain administrator privileges.

We have observed the threat actor copying malware over to systems in a compromised environment, which did not have any outbound internet access. In one of these instances, the threat actor spent more than an hour attempting to establish an outbound connection using PlugX until it realised that the host had no internet access, at which point the malware and all supporting files were deleted. APT10 achieves persistence on its targets primarily by using scheduled tasks or Windows services in order to ensure the malware remains active regardless of system reboots.

APT10 heavily leverages the shared nature of client-side MSP infrastructure to move laterally between MSPs and other victims. Systems that share access and thus credentials, from both a MSP and one of its clients serve as a way of hopping between the two.

Figure 16: Client – MSP shared infrastructure



Systems sharing credentials across the client and the MSP are of particular interest to APT10, and are commonly used by the threat actor in order to gain access to new areas of the network

13 http://csirt.ninja/?p=1103
14 http://www.meiji.ac.jp/isc/information/2016/6t5h7p00000mjbbr.html
15 http://www.chuo-u.ac.jp/research/rd/grant/news/2017/01/51783/

Figure 12. PWC Report – Initial Compromise and Lateral Movement

respectively. For example, in addition to compromising high value domain controllers and security servers, the threat actor has also been observed identifying and subsequently installing malware on low profile systems that provide non-critical support functions to the business, and are thus less likely to draw the attention of system administrators.

As part of the long-term access to victim networks, we have observed APT10 consistently install updates and new malware on compromised systems. In the majority of instances APT10 used either a reverse shell or RDP connection to install its malware; the actor also uses these methods to propagate across the network.

Communication checks are usually conducted using native Windows tools such as ping.exe, net.exe and tcping.exe. The actor will frequently 'net use' to several machines within several seconds, connecting for as little as five seconds, before disconnecting. Further details are provided in Annex B.

Network hopping and exfiltration

Once APT10 have a foothold in victim networks, using either legitimate MSP or local domain credentials, or their sustained malware such as PlugX, RedLeaves or Quasar RAT, they will begin to identify systems of interest.

The operator will either access these systems over RDP, or browse folders using Remote Access Trojan (RAT) functionality, to identify data of interest. This data is then staged for exfiltration in multi-part archives, often placed in the Recycle Bin, using either RAR or TAR. The compression tools are often launched via a remote command execution script which is regularly named 't.vbs' and is a customised version of an open source WMI command executor which pipes the command output back to the operator.

We have observed these archives being moved outside of the victim networks, either back into to the MSP environments or to external IP addresses in two methods, which are also performed via the command line using t.vbs:

1. Mounting the target external network share with 'net use' and subsequently using the legitimate Robocopy tool to transfer the data; and,

MSP or victim networks, then, using similar methods, 'pulls' the data from those networks to locations from which they can directly obtain it, such as the threat actor's C2 servers.

APT10's ability to bridge networks can therefore be summarized as:

- Use of legitimate MSP credentials to management systems which bridge the MSP and multiple MSP customer networks;
- Use of RDP to interactively access systems in both the MSP management network and MSP customer networks;
- Use of t.vbs to execute command line tools; and,
- Use of PSCP and Robocopy to transfer data.

APT10 malware

We classify APT10's malware into two distinct areas: tactical and sustained. The tactical malware, historically EvilGrab, and now ChChes (and likely also RedLeaves), is designed to be lightweight and disposable, often being delivered through spear phishing. Once executed, tactical malware contains the capability to profile the network and manoeuvre through it to identify a key system of interest. The sustained malware, historically Poison Ivy, PlugX and now Quasar provides a more comprehensive feature set. Intended to be deployed on key systems, the sustained malware facilitates long-term remote access and allows for operators to more easily carry out administration tasks.

Since late 2016, we have seen the threat actor develop several bespoke malware families, such as ChChes and RedLeaves. Additionally, it has taken the open source malware, Quasar, and extended its capabilities, ensuring the incrementation of the internal version number as it does so.

We have also observed APT10 use DLL search order hijacking and sideloading, to execute some modified versions of open-source tools. For example, PwC UK has observed APT10 compiling DLLs out of tools, such as MimiKatz and PwDump6, and using legitimate, signed software, such as Windows Defender to load the malicious payloads.

In Annex B we provide detailed analysis of several of the threat actor's tools as well as the common Windows tools we have observed being used.

Figure 13. PWC Report – Network Hopping and Exfiltration

From these sections, we can extract a rough attack path for menuPass that we describe using ATT&CK Techniques.

1. Initial Access – first, menuPass gains access to the target network, often through phishing attacks. They then deploy malware to establish a foothold.
2. Discovery – menuPass performs both local and remote discovery, gathering information about the target environment.
3. Credential Access – menuPass attempts to acquire credentials by dumping memory.
4. Lateral Movement – menuPass uses acquired credentials to move laterally to other systems within the network.
5. Persistence – menuPass establishes persistence on systems they have gained access to.
6. Discovery – using their increased access, menuPass identifies data of interest.
7. Collection – menuPass collects and stages data for exfiltration by compressing it into RAR or TAR archives.
8. Exfiltration – menuPass exfiltrates collected data by "pushing" it from target systems onto external infrastructure.

Note: A clear attack path may not always be easily found from public reports. In such an instance, it may be appropriate to use attack paths used by other adversaries, such as the one we developed above. This is because in many cases adversaries follow similar paths of attack.

Step 6: Convert Technique List to Emulation Plan

Now that we have an attack path developed, we can start fitting the techniques we've already gathered into this path. This should be relatively simple since we described the path using ATT&CK tactics.

As we've only gathered three techniques in this walkthrough, we won't be performing this step here. Instead, we'll discuss some points to note for this process for you to use.

- Some tactics may be repeated within the attack path. For example, an adversary may perform remote discovery immediately following initial compromise to understand network topology, and then perform local discovery to discover files of interest after lateral movement. This can create some complexity in assigning techniques to the attack path, but this should be solvable with additional consideration and research.
- It may be appropriate to perform the same technique in multiple phases of the emulation. While the attack path is represented in a linear format, adversary behaviors are often cyclical. Adversary campaigns can be very lengthy, and it is expected behavior for adversaries to attempt to gather information through discovery, credential access, and collection for most if not all machines they gain access to throughout their campaign, which may again be followed by further lateral movement.
- Not all of the techniques that you've found may fit neatly within the attack path you generated, and that's okay. It is not vital to strictly follow the attack path – some deviation is acceptable. Alternatively, if the technique does not fit neatly or logically in any part of the path, it may also be appropriate to leave it out entirely.
- If you are assuming a post compromise scenario, you can begin your emulation after Initial Access.

At the end of this process, you now have a serviceable Adversary Emulation Plan!

Step 7: Further Steps

Before this emulation plan can be executed, there may be additional work that is necessary. Some procedures may use malware or tools that either need to be developed or acquired. Others may not work anymore due to security patches, and so alternative procedures will need to be researched. Finally, the appropriate infrastructure is required to execute the emulation plan, including necessary (mis)configurations.

After you have a working emulation plan, you are now ready to emulate your chosen adversary! It is strongly recommended to run new emulation plans on test infrastructure before attempting them on production environments. Adversary behaviors are dangerous, and that is why we work to defend our organizations from them. You should be intimately familiar with the impacts of each of the behaviors you intend to run before executing them on production environments.

One final consideration: the Adversary Emulation community is constantly growing through research and development that is made publicly available. This is how we as Adversary Emulation Engineers work to defend against our common adversaries. Just as we used publicly available resources to create our emulation plan in this lab, publicly releasing your adversary emulation plan either through a blog post, your own Github account, or the Center for Threat Informed Defense's Adversary Emulation Library, among others, can help give back to the community.

Summary

As we saw in this lab, creating an adversary emulation plan is a time intensive task involving several steps. It isn't sufficient to know only the specific behaviors the adversary performs – you also need to understand their overall methodology to truly emulate them. When done correctly, this exercise produces a document that can provide value for years to come, both for your organization and the adversary emulation community as a whole.