CYSIV
A FORESCOUT COMPANY

Threat Report:
APT10

July 12, 2019

Table of Contents

1 EXECUTIVE SUMMARY 3
2 THREAT ACTOR GROUP "APT10" 4
3 TOOLSETS 5
4 MITRE ATT&CK MATRIX 8
5 CAMPAIGNS 9
5.1 Menu Pass 9
5.2 Cloud Hopper 9
5.3 Chess Master 9
5.4 White Fly 10
5.5 Hogfish Redleaves (New Battle) 11
5.6 Trade Secret 11
5.7 Soft Cell 12
5.8 Others 15
6 APT10'S NETWORK BEHAVIOR 16
7 IOCs 17

Table of Figures

Figure 1 Utilities used by APT10 5
Figure 2 Malware families used by APT10 6
Figure 3 Open Source tools used by APT10 7
Figure 4 Most common TTPs used by APT10 8
Figure 5 Process view 14
Figure 6 High-level view of infrastructure used in operation Cloud Hopper in 2016 16

1 EXECUTIVE SUMMARY

APT10 is a highly sophisticated advanced persistent threat (APT) group that has been active since at least 2006. APT10 is believed to be a China-based actor and has conducted several cyber espionage operations on several different organizations across different industries including Education/Research, Cloud Service Providers, Defense, Government, Healthcare, Telecommunications, Managed Service Providers (MSPs), Manufacturing, Hospitality, Aerospace and Mining. The primary intent of APT10 is stealing strategic information, such as trade secrets and intellectual propery, to achieve China's national security objectives.

This threat actor has used various malware toolsets to drive its cyber espionage operations. One of the first malware families used by APT10 was PoisionIvy RAT, which was distributed using a spear phishing attack to infect Defense organizations, especially those in the United States. Another commonly used backdoor by APT10 is PlugX. APT10 has used this backdoor to target several government agencies around the world to steal the sensitive data and send them to C&C servers. APT10 constantly checks the security research community and whenever they discover their backdoors have been open sourced, they switch their toolset to new ones. This group is known to use large interconnected dynamic domains for its C&C infrastructure, which makes the detection of infrastructure hard.

This threat report provides an overview of APT10 including its toolset and its most well-known operations.

Protection Provided by Cysiv:
The following Cysiv advanced managed security services provide protection from APT10:

- 24x7 monitoring and management provides organizations with real time alerts and quick isolation and remediation to contain a threat during the early stages of an attack to prevent a compromise, data loss or breach.
- **User Protection Service:** The anti-malware module that's deployed as part of this service constantly monitors abnormal activities in the following OS locations to detect any malicious behavior:
  - Master Boot Record (MBR)
  - Files
  - Registry entries
  - Kernel code patches
  - Operating system service hooks
  - File streams
  - Drivers
  - Ports

- Processes
- Services

- **Advanced Threat Detection Service:** Network security appliances deployed and monitored as part of this service detect phishing attacks/attachments, and are able to identify C&C communication over any port, and over 100 protocols. These appliances also provide custom sandboxing, which can be used to detonate any suspicious files and executables to help prevent a breach.
- **Hybrid Cloud Security Service:** Anti-malware provides protection from APT10 malware toolsets, and application control detects and optionally prevents the execution of unknown binaries, depending on how it's configured (detect mode or block mode).

2 THREAT ACTOR GROUP "APT10"

APT10 is an advanced persistent threat group that many industry experts believe is from China that has been active since approximately 2006. They have been on the radar of different security companies, and are known by different code names: APT10 (FireEye), Red Apollo (PWC), CVNX (BAE Systems), Stone Panda (CrowdStrike), MenuPass (Trend Micro), Happyyongzi, POTASSIUM, DUSTSTORM, HOGFISH, CLOUDHOPPER. For the purposes of this report, FireEye's naming has been used as it was the security company that first introduced this threat actor publicly, and as such most people know this APT by "APT10".

According to US officials, the primary purpose of many of the group's campaigns is to steal trade secrets and intellectual property that the Chinese government then passes to local Chinese companies, helping create unfair advantage for local firms on the global market.

During the years of operations, the threat actor targeted several organizations in several different industries. The primary target industries of this APT are Education/Research, Cloud Service Providers, Defense, Government, Healthcare, Telecommunications, Managed Service Providers (MSPs), Manufacturing, Hospitality, Aerospace and Mining.

The targets of this group have included United States, Australia, Canada, Japan, New Zealand, Germany, India, South Africa, South Korea, Sweden, France, Finland, United Kingdom, Brazil, Thailand, Switzerland and Norway.

The most common initial attack vector used by APT10 is spear phishing, in which the actor usually leveraged .lnk file within archives. In addition to this method, this APT has used another method in which it is infecting its victims through global/managed service providers (MSPs). Since the MSPs have significant access to their clients' network, APT10 starts its attack by compromising the MSP's network to move laterally into the network of the MSP's clients. The actor also can take advantage of network traffic between the MSP's client and the MSP itself, to exfiltrate data stealthily. This is because network traffic between the MSP's client and MSP is usually considered to be benign by the client's security team.

3 TOOLSETS

APT10 constantly creates, maintains and updates different types of malware and toolsets. Figure 1, Figure 2 and Figure 3 provide the list of toolsets used by this group.

Figure 1 Utilities used by APT10

Tool Name	Description
certutil	Certutil is a Windows command line utility that can dump and display certification authority (CA) configuration information and configure certificate services. APT10 has used this tool to decode binaries hidden inside certificate files as Base64 information. It also has been used to download files from a given URL.
cmd	Cmd is a Windows command line utility that is used to locate, execute, copy and delete files into local or remotely connected victim.
Net	The Net command is a command line utility that can be used to manage network settings including network shares, network services, network users, and network connections.
Ping	Ping is the network software utility that has been used to discover remote systems within a network.
PsExec	PsExec is a light-weight Microsoft tool that executes processes on other systems, complete with full interactivity for console applications, without having to manually install client software.

Figure 2 Malware families used by APT10

Tool Name	Type	Description
ChChes (Scorpion, Haymaker)	Trojan	This is a Trojan that has been used exclusively by APT10 and acts as a system fingerprinting utility. It uses HTTP to communicate to its C&C server. Even though it can execute just a few functions by itself, its functionality can be extended by receiving modules from C&C servers and loading them into memory.
EvilGrab	Trojan	EvilGrab is a Trojan that has the capability to capture the audio, video and screen of the victims and send them to C&C servers. It has common reconnaissance capabilities such stealing credentials, instant messaging chat logs, keystrokes and also has the capability to access to the victims' machines remotely.
PlugX (Sogu)	RAT	Plugx is a modular RAT that can execute a wide variety of commands, including uploading and downloading files, and spawning a reverse shell. The malware can be configured to use multiple network protocols to avoid network-based detection. DLL side loading is often used to maintain persistence on the compromised system.
PoisonIvy	RAT	PoisionIvy is a RAT that opens a backdoor on the compromised computer and has keylogging capabilities. The RAT is controlled through a familiar Windows interface and offers several features: key logging, screen capturing, video capturing, file transfers, password theft, system administration, traffic relaying, and more.
RedLeaves (Bugjuice)	RAT	The RedLeaves implant is a remote administration trojan (RAT) that is built in Visual C++ and contains a number of functions typical of RATs, including system enumeration, command execution, command window generation and network traffic compression and encryption. The backdoor communicates over TCP using a custom binary protocol to communicate with its C&C. It also can use HTTP and HTTPs if directed by the C&C.
Snugride	Back door	This backdoor is usually used as the first stage backdoor by APT10 and has several capabilities such as taking a system survey, access to the filesystem, executing commands and a reverse shell. Its C&C communication is over HTTP and encrypted using AES with static key.
Uppercut	Back door	This is another backdoor used by APT10 that is also known as ANEL. It has ability to collect information on the victim's machine and send the infected environment's information to the C&C server. When sending the information, Uppercut encrypts the data using blowfish, XOR, and Base64-based encryption methods. The format this backdoor uses to send data is similar to ChChes, but its encryption method is easier to use.
Scanbox	Re-conn-aiss-ance Frame work	Scanbox is a reconnaissance framework used by several Chinese APT groups, including APT10, that enables attackers to track visitors to compromised websites, performs keylogging, and harvest data that could be used to enable follow-on compromises. It has the capability to deliver secondary malware on targeted hosts.

Figure 3 Open Source tools used by APT10

Tool Name	Type	Description
Mimikatz	Info Stealer	Mimikatz is an open-source application that is designed to steal credentials.
Power Sploit	Offensive security framework	PowerSploit is an open source penetration testing framework comprises of a collection of Microsoft PowerShell modules that can perform code execution, persistence, bypassing anti-virus, recon, and exfiltration.
Pwdump	Credential Dumper	This utility dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file.
Impacket	Net-working tool	Impacket is a collection of Python classes for working with network protocols. It has several capabilities such as remote service execution, Kerberos manipulation, Windows credential dumping, packet sniffing, and relay attacks.
Quasar	Rat	Quasar is an open source RAT that has a built-in keylogger to monitor mouse and keyboard events. It also has the capability to steal credentials from browsers and FTP clients and launch a remote shell to execute commands on the victim's machine.

4 MITRE ATT&CK MATRIX

Here is the list of the most common TTPs used by APT 10, based on the MITRE ATT&CK matrix.

Figure 4 Most common TTPs used by APT10

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Cre-dential Access	Discovery	Lateral Movement	Collection	C&C	Exfiltration	Impact
Spearphi shing Attach-ment	Windows Management Instrumentati on	DLL Search Order Hijacking	DLL Search Order Hijacking	Deobfuscate /Decode Files or Information	Credenti al Dumping	System Network Connections Discovery	Remote Desktop Protocol	Data from Local System	Connec tion Proxy	Data Compressed	
Trusted Relations hip	PowerShell	Valid Accounts	Scheduled Task	DLL Search Order Hijacking	Input Capture	System Network Configuration Discovery	Remote File Copy	Data from Network Shared Drive	Standar d Crypto Protoco ls	Data Encrypted	
	Scheduled Task		Process Injection	DLL Side-Loding		Remote System Discovery	Remote Services	Data Staged			
	Scripting			File Deletion		Network Service Scanning		Input Capture			
	User Execution			Masqueradin g		Account Discovery		Clipboard Data			
	Command-Line Interface			Obfuscated Files or Information							
	Execution Through API			Process Hollowing							
				Scripting							
				Valid Accounts							

5 CAMPAIGNS

In the past few years, APT10 has conducted several campaigns around the globe that has stolen sensitive data from millions of people. The following sections analyze campaigns that have been operated by APT10.

5.1 Menu Pass

The “Menu Pass” attack has been active from 2009 to 2013, with a spike in 2012. It targeted the defense industry and international government agencies, and attempted to steal military intelligence. In this campaign, spear phishing emails used attachments, which were meant to look like a purchase order or price quote that would be fairly specific to the victim, were infected with PoisonIvy.

5.2 Cloud Hopper

One of the most interesting APT10 campaigns that happened between late November 2016 and early 2017 was called “ClouldHopper”. In this campaign, the actor targeted several Managed Service Providers (MSPs) and was able to get access to the intellectual property and sensitive data of those MSPs and their clients globally. At the time, they also targeted several Japanese organizations.

In this campaign, APT10 switched its attack vector to target MSPs because this allowed them to move laterally over the MSP network to the MSP’s client’s network. In this way, by infecting an MSP they could access a large number of MSP customers. Moreover, the actor exfiltrated the MSP’s client’s data stealthy by misusing the trust communication between MSP’s network and MSP’s client’s network.

PlugX, RedLeaves, Quasar Rat, Mimikatz, nbtscan and Pwddump have been used to perform APT10 operations. In this campaign, Redleave was used as a first stage light weight backdoor that was delivered via a spear phishing attack. After gathering initial information about the targets, which was collected by Redleave, the actor used PlugX and Quasar, which have a comprehensive feature set that is required to collect required info.

5.3 Chess Master

ChessMaster is another campaign operated by APT10 in July 2017 targeting Japanese academic, technology, media and MSP companies, and government agencies. It

employed spear-phishing emails containing decoy document to infect victims. In this campaign APT10 used a variety of tools and techniques such as:

- **TinyX:** A variant of PlugX backdoor with a modular structure that allowed it to adopt new capabilities. It was bundled separately in spear-phishing emails.
- **ChChes:** ChChes backdoor was used as a second-stage payload that used different encryption methods and C&C communications.
- **RedLeaves:** RedLeaves is another second stage backdoor used in this campaign that operates like the open-source and fileless remote access trojan (RAT) Trochilus, which is known for enabling lateral movement in the infected systems.
- **Runtime packers:** The second stage backdoor, ChChes, employed three packers to obfuscate itself and avoid detection:
    - Packer without encryption
    - Packer that employed anti-emulation XOR encryption technique
    - The packer employed an AES algorithm on top of XOR encryption
- **Malicious shortcut (LNK) files and PowerShell:** LNK files have been used as an attachment of spear phishing emails. Upon opening the LNK file, it executed a Command Prompt that downloads a PowerShell script, which would either directly drop or reflectively load ChChes into the machine to make ChChes a fileless malware.
- **Self-extracting archive (SFX):** APT10 in the campaign used SFX archine five to employ its DLL hijacking method. SFX archive dropped an executable (EXE), a dynamic-link library (DLL), and a binary file (.BIN). Upon their extraction, malicious code was injected into the process of a legitimate file/application (DLL hijacking).
- **Hacking Tools:** Email and browser password recovery and dumping tools have been used in this campaign. These tools had the capability to restore forgotten passwords and use for lateral movement.

5.4 White Fly

In July 2018, SigHealth, the largest healthcare organization in Singapore, was targeted by APT10. Symantec reported this attack and called it WhiteFly. APT10 remained within the targeted organization for a long period of time and were able to steal 1.5 million patient records. Several variants of PlugX backdoor, Mimikataz, and a new RAT called Vcrodat were used by the actor in this campaign.

The attack started by sending phishing emails that pretended to offer information on job openings or appear to be documents sent from another organization operating in the same industry, to the victim. The document or image contained a malicious executable dropper that dropped the Vcrodat backdoor using the DLL search order hijacking technique. This is the same technique usually used by this APT to lunch PoisonIvy backdoor.

Once executed, Vcrodat loaded an encrypted payload on to the victim's computer. This backdoor collected the system information about the infected computer and sent them to the C&C server. It also had the capability to download additional tools. After collecting the information, APT10 used a second piece of custom malware that Symantec labeled "Trojan.Nibatad", a variant of PlugX, to exfiltrate the stolen data.

5.5 Hogfish Redleaves (New Battle)

On May 2018 researchers reported a new APT10 operation called "HogFish RedLeaves", which attacked several Japanese organizations. In this campaign, APT10 used its favorite method to infect victims: sending phishing emails which dropped the RedLeave backdoor. The variant of Redleave used in this attack had the following capabilities:

- Take screenshots
- Gather browser usernames and passwords
- Gather extended system information
- Send, receive, and execute commands from the C&C server (RedLeaves will attempt to communicate over HTTP, using POST requests with a hardcoded User-Agent)

5.6 Trade Secret

In Feb 2017, security researchers observed a strategic web compromise on a prominent U.S. lobbying group that served up malware to target key private-sector players involved in lobbying efforts around United States foreign trade policy. At the same time, the attacker launched a similar attack against Japan's government officials.

In this operation, named Trade Secret, visitors to compromised websites, which are used to register for specific meetings at the National Foreign Trade Council, were infected by Scanbox malware framework.

Scanbox is a framework written in JavaScript and PHP that allows an attacker to perform reconnaissance and key logging of visitors to a compromised website without requiring any malware to be downloaded or installed. Here is list of scanbox plugins:

- Applications enumeration
- Browser info reconnaissance
- Adobe Flash reconnaissance
- SharePoint reconnaissance
- Java versions enumeration
- JavaScript keylogger
- Microsoft Office reconnaissance
- Network reconnaissance

5.7 Soft Cell

In 2018, a group of researchers identified an advance persistent campaign that targeted several global telecommunications providers. Evidence suggests that this campaign has been active since 2012. The campaign goal was to obtain CDR records of a large telecommunications provider.

Based on techniques, tactics and procedures used in this campaign, the researchers associated this campaign to APT10. This attribution is relative, and it could be the work of other similar Chinese APTs such as Deep Panda. The campaign continued for several months and had four stages. In the first stage of attack, APT compromised a public vulnerable web server with a web shell from which the attackers gathered information about the network and propagated across the network. The threat actor was able to leverage the web shell to run reconnaissance commands, steal credentials, and deploy other tools. Upon detection by security teams, the attackers stopped its operations for a few months.

The second stage of attack happened four months later in which the attacker used similar set of tools and techniques as those used in stage one. Again, as malicious activity was detected and remediated against, the threat actor stopped the attack. The process of resuming, and stopping upon detecting, happened two more times.

During this operation, the attacker used several toolsets and techniques:

- Several custom web shells were used to run reconnaissance commands, steal credentials, and deploy other tools.

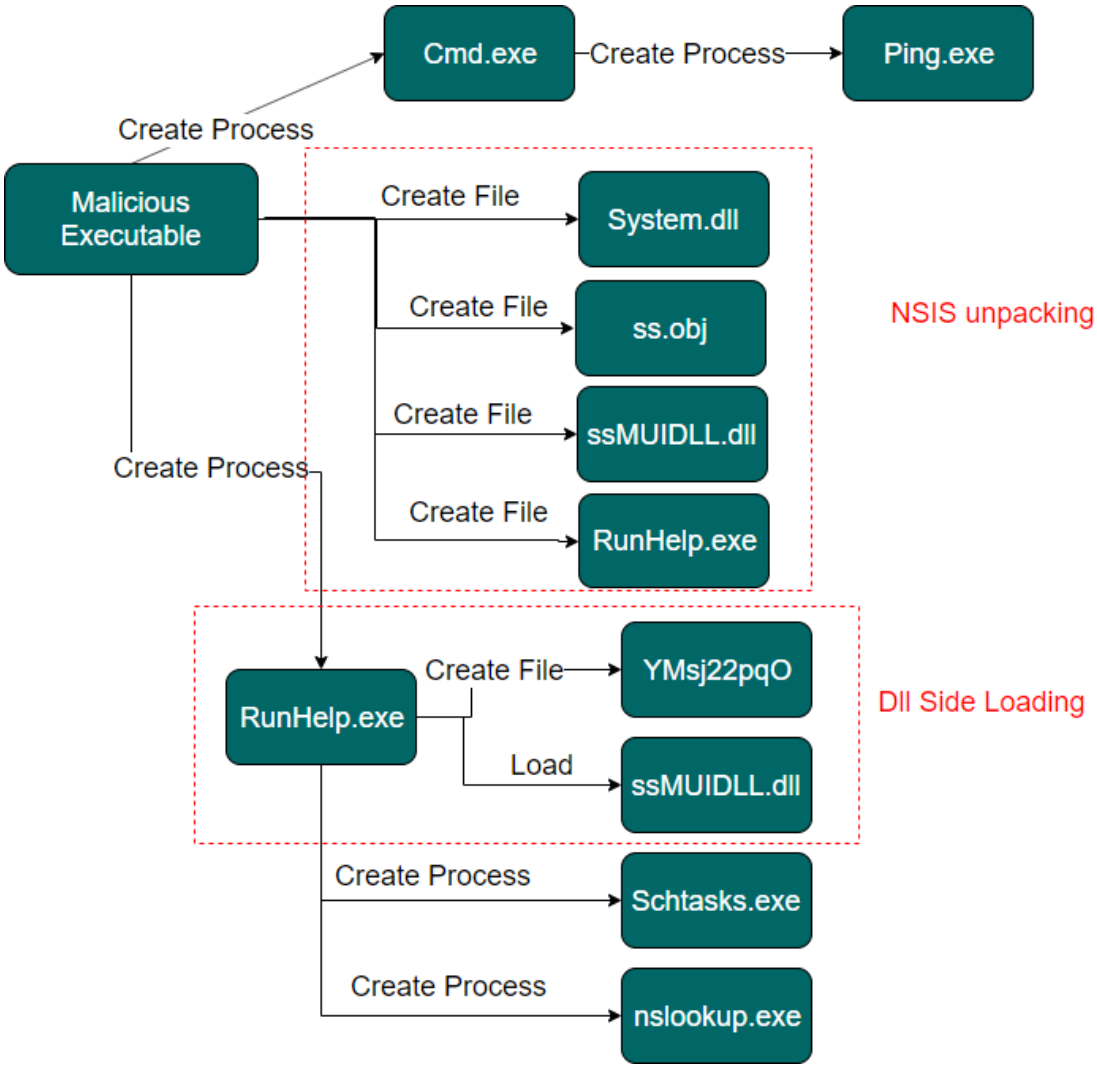
- Several enumeration commands were used to obtain and enumerate information about the compromised machines, network architecture, users, and active directory enumeration.
- A modified version of nbtscan was used to identify available NetBIOS name servers locally or over the network.
- A modified version of Mimikatz was used to dump credentials stored on the compromised machines. This version of mimikatz did not require any command line arguments, most likely in an attempt to avoid detection based on command-line auditing.
- The actor also used another technique that dumped specific hives from the Windows Registry, such as the SAM hive, which contains password hashes.
- It used WMI and PsExec to move laterally over the network.
- In order to maintain a long-term foothold and stealing information, the APT group abused the stolen credentials to create rogue, high-privileged domain user accounts, which they then used to take malicious action.
- The actor used a variant of PoisonIvy to maintain access across the compromised assets and steal information on the infected hosts. PoisonIvy is a powerful, multi-featured RAT that lets a threat actor take total control over a machine and has the following features:
    - Registry Editor
    - 1Screenshot Grabber
    - Credential Stealer
    - Interactive Shell
    - File Manager with Upload and Download Support
    - Process Monitor
    - Keylogging and Various other Surveillance Features

5.7.1 OVERVIEW OF POISIONIVY

The variant of poisonIvy used in this attack is a Nullsoft Scriptable Install System (NSIS) that employed a DLL side-loading technique to stealthily load itself into memory. To do this, it exploited a legitimate signed application, in this case Runhelper.exe, which is a legitimate signed Samsung tool, to load the PoisonIvy payload into memory. NSIS installer is an archive file includes Runhelper.exe and a fake DLL with the same name as a legitimate DLL (ssMUIDLL.dll), which is required by the application. After the fake DLL was loaded by the Runhelper.exe, it decrypted a payload in the same folder, which

contains the actual PIVY payload. Then it made itself persistent by creating a scheduled task. The behavioral process graph of this backdoor is shown in Figure 5.

Figure 5 Process view



5.8 Others

Besides the major operations that APT10 conducted, they also attacked several individuals, universities and other organizations:

- According to several reports, the Marriot International breach on November 2019 that resulted in the theft of data from 500 Million guest, was the operation of APT10. The attackers targeted the Starwood guest reservation database, which contained details of reservations that were made on or before 10 September 2018. The most discerning revelation of the Marriott investigation is that the hackers gained access to the Starwood network, back in 2014 without being detected. Still, there's no information about the malware family that was used by APT10 in this campaign.
- APT10 also targeted the Japanese media sector in July 2018. In this attack, the actor used spear phishing as its initial infection vector to install Uppercut backdoor.
- In October 2016, APT10 attacked several Japanese organizations using ChChes backdoor.
- Between November 2017 and September 2018, APT10 targeted at least three companies in the United States and Europe, including:
    - Visma: A Norwegian IT and business cloud services MSP that has at least 850k customers globally
    - An international apparel company
    - A U.S law firm

  Interestingly, in this campaign, attackers gained access to victim networks via deployments of Citrix and LogMein remote-access, using stolen valid user credentials, and then they conducted enumeration and privilege escalation on the targeted networks. To deploy the malware on the victims, they used the DLL side loading technique. RedLeaves and Uppercut have been used by APT10 in this campaign. The stolen data was compressed using WinRAR and then exfiltrated to a Dropbox account using cURL.
- One of the most recent APT10 campaigns was uncovered by Ensilo researchers on May 24, 2019. In this attack, the actor targeted organizations in South East Asia. Similar to its previous campaigns, it employed some specific variants of PlugX and Quasar rat that were loaded into memory using DLL side loading technique.

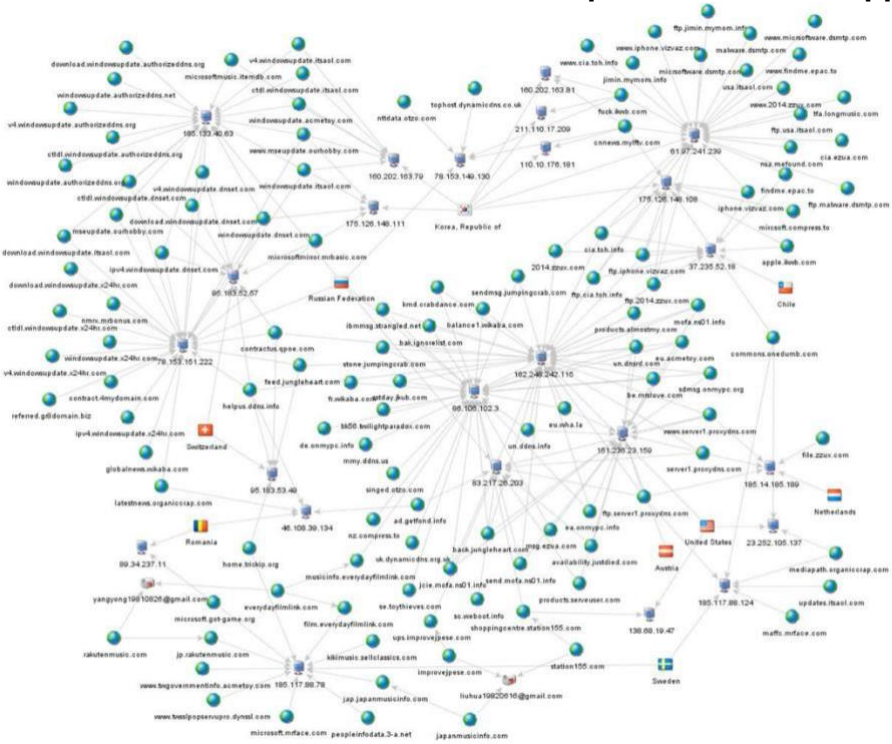
6 APT10’S NETWORK BEHAVIOR

APT10 malware toolset is known to use different protocols for their C&C communications. They usually are capable of performing communication over TCP using DNS, HTTP and HTTPS. The server is able to change type of C&C communications on the infected host.

The C&C infrastructures used by APT10 in its campaigns are based on dynamic domains. They employed lots of highly interconnected domains through shared IP address hostings that sometimes linked back historically to the actor’s previous operations.

For example, in operation Cloud Hopper they employed thousands of dynamic domains in their infrastructure. To give you an idea of its size, Figure 6 shows the high-level view of this infrastructure in the Cloud Hopper operation of 2016 provided, by PWC. As the campaign progressed into 2017, the number of dynamic domains increased significantly.

Figure 6 High-level view of infrastructure used in operation Cloud Hopper in 2016



7 IOCS

The list of IOCs' is available in a separate CSV file.

Cysiv provides advanced cyber risk management as a service to enterprises that need to better defend themselves from breaches, and demonstrate they are upholding their fiduciary duty of care.

We combine 24x7x365 access to an elite team of security and threat experts, global cyber intelligence, an AI-powered security and operations analytics platform, and market-leading integrated security technologies to extend and elevate your security capabilities and posture.

www.cysiv.com

Aligned with how you want to consume IT, Cysiv allows you to pay monthly, based on the security services you consume, and can scale rapidly to support your business needs.

Cysiv is a partnership between Trend Micro Incorporated, a global leader in cybersecurity solutions, and HITRUST, a leader in cyber security and information risk management. Together, they enable Cysiv to offer organizations a better approach to cyber risk management.