TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

02 JAN 2019

Alert Number

AB-000102-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Chinese APT10 intrusion activities target Government, Cloud-Computing Managed Service Providers and Customer networks worldwide.

The following information was obtained through FBI investigations and is provided in accordance with the FBI's mission and policies to prevent and protect against federal crimes and threats to the national security.

The FBI is providing the following information with **HIGH confidence**:

SUMMARY:

The FBI obtained information regarding a group of Chinese APT cyber actors stealing high value information from commercial and governmental victims in the U.S. and abroad. This Chinese APT group is known within private sector reporting as APT10, Cloud Hopper, menuPass, Stone Panda, Red Apollo, CVNX and POTASSIUM. This group heavily targets managed service providers (MSP) who provide cloud computing services; commercial and governmental clients of MSPs; as well as defense contractors and governmental entities. APT10 uses various techniques for initial compromise including spearphishing and malware. After initial compromise, this group seeks MSP administrative credentials to pivot between MSP cloud networks and customer systems to steal data and maintain persistence. This group has also used spearphishing to deliver malicious payloads and compromise victims.

In addition to and through cloud-computing MSPs, APT10 targets victims in the following areas:

- Agriculture
- Automotive
- Defense contractors
- Electronics
- Energy
- Financial
- Government
- Human Resources
- Manufacturing
- Medical
- Military
- Mining
- Shipping
- Technology services
- Telecommunications

Any activity related to APT10 detected on a network should be considered an indication of a compromise requiring extensive mitigation and contact with law enforcement.

The FBI is providing the following information with **HIGH confidence**:

TECHINICAL DETAILS:

APT10 uses custom tools which should be immediately flagged if detected, reported to FBI CYWATCH, and given highest priority for enhanced mitigation. The presence of such tools is typically part of a comprehensive, multifaceted effort to maintain persistent network access and exfiltrate data. The custom tools used by this group are as follows:

REDLEAVES

The REDLEAVES implant is a remote access Trojan (RAT) which operates largely in memory with functionality suitable for system enumeration and lateral movement within victim networks. Industry reporting provides REDLEAVES may be used in spearphishing campaigns as an intrusion vector. REDLEAVES source code shares

commonalities with TROCHILUS RAT. Variants of REDLEAVES include HIMAWARI and LAVENDER malware.

REDLEAVES comprises an executable file (EXE), custom loader (DLL) and an encoded data file (DAT) containing shellcode and the REDLEAVES DLL. Upon execution of the EXE file, the custom loader DLL is side-loaded and conducts a function call to load and decode an XOR encoded data file containing (a) stage-one shellcode, (b) stage-two shellcode and (c) the REDLEAVES DLL. The stage-one shellcode launches "svchost.exe" to process hollow the stage-two shellcode; stage-two shellcode, in turn, allocates memory in "svchost.exe" to load REDLEAVES DLL. After the REDLEAVES DLL runs, the EXE file process terminates.

REDLEAVES is able to utilize a named pipe to execute commands in remote shell or, alternatively, pass instructions through "cmd.exe" to execute commands directly in the command shell. Basic REDLEAVES functionality includes victim system enumeration, file search/deletion, screenshots, as well as data transmission. Prior to transmission, REDLEAVES compresses raw data with MiniLZO and encrypts said data with RC4 encryption. REDLEAVES is able to communicate with command and control (C2) servers on HTTP/HTTPS or custom TCP protocols across ports 53, 80, 443 and 995.

Although REDLEAVES operates in memory to avoid detection, early versions may not conduct anti-forensics; evidence, therefore, of files copied to/from an infected host may still be present on disk. If a machine is believed to be infected, it is recommended to examine for "svchost.exe" processes which do not have "services.exe" as parent; "svchost.exe" memory pages mapped as read-write-execute (RWX); as well as reviewing forensic memory capture for anomalies commonly associated with malicious processes.

UPPERCUT/ANEL

UPPERCUT, also known as ANEL, is a backdoor Trojan used in spearphishing campaigns to deploy second-stage payloads such as credential harvesters. Industry reporting states APT10 deploys UPPERCUT through decoy Word documents containing a malicious Visual Basic macro (VBA). UPPERCUT is known to exploit CVE-2017-

8759 and CVE-2017-1182. It may be detected by antivirus engines as "TROJ_ANELLDR", "BKDR_ANELENC", "APT.Backdoor.Win.UPPERCUT" and/or "FE_APT_Backdoor_Win32_UPPERCUT".

Installation commences when the victim user enables the Word document macro, resulting in the download of three Privacy Enhanced Mail (PEM) text files. These PEM files are decoded with "certutil.exe" to produce an EXE, DLL and DAT containing shellcode and the UPPERCUT DLL. Upon execution of the EXE file, the custom loader DLL is side-loaded and conducts a function call to load and decrypt the shellcode; the shellcode decodes and decompresses the UPPERCUT DLL. After the UPPERCUT DLL runs in memory, the PEM files are deleted with "esentutle.exe".

UPPERCUT is known to use Blowfish encryption when communicating with C2 servers. UPPERCUT communicates with C2 servers through HTTP GET or POST requests. UPPERCUT initially collects victim computer information, such as hostname and OS version, and then aggregates and encrypts the data into a string embedded within the Uniform Resource Identifier (URI) of HTTP requests. Upon receiving an initial request, the C2 server will respond with an HTTP status response; if no C2 response is given, UPPERCUT may resend the HTTP request with a "GetLastError" code contained within the Cookie header. Subsequent commands and modules between the C2 servers and UPPERCUT are Blowfish encrypted and then embedded within the body of HTTP requests or responses. Basic functionality includes the ability to execute commands, upload/download files, load executables and take screenshots.

CHCHES

CHCHES, also known as CHINESE CHESS, is a RAT which communicates with C2 servers using HTTP Cookie headers. Industry reporting provides CHCHES may be used in spearphishing campaigns as an initial intrusion vector designed to deploy second-stage payloads. The CHCHES EXE is known to disguise itself with a Word icon or shortcut, as well as use expired or revoked certificates.

CHCHES initially collects victim computer hostname; process identifier (PID); current working directory (%TEMP%); screen resolution; as well as kernel32.dll or explorer.exe version. This data is aggregated into a string, encrypted and embedded within the Cookie header of an HTTP GET or POST request and beaconed to a C2 server. The C2 server responds with a HTTP status response containing a unique identifier within the "Set-Cookie" tag. After a second HTTP GET beacon is sent containing the unique identifier encrypted and embedded within the Cookie header, the C2 server will transmit modules and commands. CHCHES modules loaded onto memory include the ability to execute commands, upload/download files, load and run DLLs, as well as encrypt communications using AES encryption.

APT10 also acquires legitimate credentials and uses commonly available tools as part of their effort to maintain persistent network access. Mitigation efforts should also focus on identifying such access and removing it. FBI has identified the following specific, but not wholly exclusive, malware and tools previously used by this group:

- QUASAR RAT

Please see APPENDIX A and APPENDIX B for technical indicators and indicators of compromise (IOCs) associated with this APT.

RECOMMENDED STEPS FOR INITIAL MITIGATION:

The FBI recommends the following mitigation measures be taken within the first 72 hours of detection:

Prepare Your Environment for Incident Response

- Establish Out-of-Band Communications methods for dissemination of intrusion response plans and activities, inform network operations centers (NOCs) and computer emergency response teams (CERTs) according to institutional policy and SOPs
- Maintain and actively monitor centralized host and network logging solutions after ensuring all devices have logging enabled and their logs are being aggregated to those centralized solutions
- Disable all remote (including remote desktop protocol and virtual private network) access until a password change with two-factor authentication has been completed
- Implement full secure socket layer (SSL) / transport layer security (TLS) inspection capability (on perimeter and proxy devices)
- Monitor accounts and devices determined to be part of the compromise to prevent reacquisition attempts
- Collect forensic images including memory capture of devices determined to be part of the compromise.

Implement core mitigations to prevent re-exploitation (within 72 hours)

Implement a network-wide password reset with two-factor authentication (preferably with local host access only, no remote changes allowed) to include:

- All domain accounts (especially high-privileged administrators)
- Local Accounts
- Machine and System Accounts

Patch all systems for critical vulnerabilities:

A patch management process which regularly patches vulnerable software remains a critical component in raising the difficulty of intrusions for cyber operators. While a few adversaries use zero-day exploits to target victims, many adversaries still target known vulnerabilities for which patches have been released, capitalizing on slow patch processes and risk decisions by

network owners not to patch certain vulnerabilities or systems. A few of these targeted vulnerabilities include the following:

- CVE-2018-8477
- CVE-2018-8514
- CVE-2018-8580
- CVE-2018-8595
- CVE-2018-8596
- CVE-2018-8598
- CVE-2018-8616
- CVE-2018-8621
- CVE-2018-8622
- CVE-2018-8627
- CVE-2018-8637
- CVE-2018-8638
- CVE-2018-8373
- CVE-2018-8174
- CVE-2017-8759
- CVE-2017-1182
- CVE-2017-0199

While watching for infections from the malware families detailed above, we also recommend ensuring you are patched against older vulnerabilities commonly exploited by cyber operators, such as CVE-2012-0158.

After initial response activities, deploy and properly configure a mitigation tool kit such as Microsoft's Enhanced Mitigation Experience Toolkit (EMET). EMET employs several mitigations techniques to combat memory corruption techniques. It is recommended all hosts and servers on the network implement mitigation toolkits.

DHS Cybersecurity and Infrastructure Security Agency Mitigation Guidance:

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has multiple alerts and additional mitigation guidance related to this APT and managed service providers. This information can be found at: https://www.us-cert.gov/china

National Security Agency Cybersecurity:

The NSA has Cybersecurity Advisories and Operational Risk Notices (ORNs), guidance, and other cybersecurity advice on their Cybersecurity website. This includes Info Sheet: Cloud Security Basics (August 2018) and Tech Report: NSA/CSS Technical Cyber Threat Framework v2 (November 2018). These can be found at: https://www.nsa.gov/what-we-do/cybersecurity/

REPORTING NOTICE:

Please report any compromise believed to be attributable to this APT group by calling or emailing FBI's 24/7 Cyber Watch (CyWatch). CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov.

When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's national Press Office at npo@ic.fbi.gov or (202) 324-3691.

ADMINISTRATIVE NOTE

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.
For comments or questions related to the content or dissemination of this product, contact CyWatch.

APPENDIX A – TECHNICAL INDICATORS

(I.) REDLEAVES:

REDLEAVES configuration block structure overview (XOR encoded).

| *C2 Domain/IP* | *Port 995, 80, 53, 443* | *HTTP/HTTPS/TCP* | *GroupID* | *Mutex* | *RC4 encryption key* |

- RC4 encryption is used in conjunction with MiniLZO for compression of raw data
- known RC4 key: 0x6A6F686E3132333400

REDLEAVES C2 communication structure overview (TCP).

Packet_01 (12 bytes):

0	4	8	C
generated 32-bit value	*FIXED 32-bit value*	*total length of second packet*	

Packet_02 (12 bytes):

0	4	8	C
uncompressed data length	*compressed data length*	*FIXED 32-bit value*	*encrypted & compressed data*

- Packet_02 headers may be XOR encoded with first four bytes of key

REDLEAVES sample, variant and/or artifact hash values.

MD5 hash: 6a1c14d5f16a07bef55943134fe618c0
Certificate: 01 00 00 00 00 01 2A 60 4F B6 B4 [Tsingsoft Imagination Information Technology Co., Ltd.]
Certificate: 04 00 00 00 00 01 1E 44 A5 EC BE [not time valid]
Certificate: 04 00 00 00 00 01 23 9E 0F AC B3 [not time valid]

MD5 hash: 81df89d6fa0b26cadd4e50ef5350f341

MD5 hash: b3139b26a2dabb9b6e728884d8fa8b33

MD5 hash: 06b0af6ff00647f57119d8a261829f73

MD5 hash: 080f8017607bb14e0b1ad25ec6e400f5

MD5 hash: 265cf3ddc1e43449ae067e0e405ecd2f

MD5 hash: 4f1ffebb45b30dd3496caaf1fa9c77e3

MD5 hash: 627b903657b28f3a2e388393103722c8

MD5 hash: 797b450509e9cad63d30cd596ac8b608

MD5 hash: c9460df90bd8db84428b8c4d3db1e1e1

MD5 hash: c9e7710e9255e3b17524738501fa8d45

MD5 hash: d2d086f62f3fcdc5be8eba3879e04b90

MD5 hash: dd0494eb1ab29e577354fca895bec92a

MD5 hash: ddc8df45efe202623b3c917d766c9317

MD5 hash: e2627a887898b641db720531258fd133

MD5 hash: ed65bbe9498d3fb1e4d4ac0058590d88

MD5 hash: fb0c714cd2ebdcc6f33817abe7813c36

(II.) UPPERCUT/ANEL:

UPPERCUT/ANEL C2 communication structure overview.

(1.) HTTP GET Request beacon URI:

GET */page/?encrypted string of victim computer data*

Structure of URI string (decrypted):

?| *generated_string_01* |=| *data_01* |&| *generated_string_02* |=| *data_02* |&| . . . |&| *generated_string_X* |=| *data_X* |

- String is Blowfish, XOR, Base64 encrypted
- Known Blowfish key: this is the encrypt key
- Known Blowfish key: f12df6984bb65d18e2561bd017df29ee1cf946efa5e510802005aeee9035dd53

(2.) C2 HTTP Response:

HTTP/1.1 200 OK . . . *Body contains Blowfish-encrypted commands and modules*

UPPERCUT/ANEL sample, variant and/or artifact hash values.

MD5 Hash: 4f83c01e8f7507d23c67ab085bf79e97

MD5 Hash: cca227f70a64e1e7fcf5bccdc6cc25dd

MD5 Hash: f188936d2c8423cf064d6b8160769f21

(III.) CHCHES:

CHCHES C2 communication structure overview.

(1.) HTTP GET Request beacon Cookie:

GET /*generated value*.htm HTTP/1.1 Cookie: *encrypted string of victim computer data*

Structure of Cookie string (decrypted):

A| *hostname* |*| *PID* |?| *FIXED value* |?| *temp folder path* | *ChChes version* |(| *screen resolution* |)|*| *kernel32.dll/explorer.exe version* |

- known fixed value: 3618468394

(2.) C2 HTTP Response:

HTTP/1.1 200 OK Set-cookie: tag= *16 byte ID of infected host (middle 16 bytes of MD5 hash value based on hostname * PID)*

(3.) HTTP GET Request reply:

GET /*generated value*.htm HTTP/1.1 Cookie: *encrypted* B| *16 byte ID of infected host* |

CHCHES sample, variant and/or artifact hash values.

MD5 Hash: 19610f0d343657f6842d2045e8818f09

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]

Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7

Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: 1d0105cf8e076b33ed499f1dfef9a46b

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: 472b1710794d5c420b9d921c484ca9e8

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: 684888079aaf7ed25e725b55a3695062

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: ca9644ef0f7ed355a842f6e2d4511546

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: 37c89f291dbe880b1f3ac036e6b9c558

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: c0c8dcc9dad39da8278bf8956e30a3fc

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: b0649c1f7fb15796805ca983fd8f95a3

MD5 Hash: 1b891bc2e5038615efafabe48920f200

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: f5744d72c6919f994ff452b0e758ffee

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: f586edd88023f49bc4f9d84f9fb6bd7d

MD5 Hash: 0c0a39e1cab4fc9896bdf5ef3c96a716

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: 23d03ee4bf57de7087055b230dae7c5b

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: c1cb28327d3364768d1c1e4ce0d9bc07

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: db212129be94fe77362751c557d0e893

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: 07abd6583295061eac2435ae470eff78

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: 7891f00dcab0e4a2f928422062e94213

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: 8a93859e5f7079d6746832a3a22ff65c

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: 3afa9243b3aeb534e02426569d85e517

Certificate: 3F FC EB A8 3F E0 0F EF 97 F6 3C D9 2E 77 EB B9 [not time valid, revoked]
Certificate: 52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7
Certificate: 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A

MD5 Hash: dbb867c2250b5be4e67d1977fcf721fb

MD5 Hash: d1bab4a30f2889ad392d17573302f097

MD5 Hash: f03f70d331c6564aec8931f481949188

MD5 Hash: 75500bb4143a052795ec7d2e61ac3261

MD5 Hash: 3cbb5664d70bbe62f19ee28f26f21d7e

MD5 Hash: ac725400d9a5fe832dd40a1afb2951f8

MD5 Hash: c2a07ca21ecad714821df647ada8ecaa

MD5 Hash: e8f3790cfac1b104965dead841dc20b2

REPORT REFERENCES

Accenture Security; HOGFISH RedLeaves Campaign; https://www.accenture.com/t20180423T055005Z_w_/us-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf

BAE Systems; APT10 – Operation Cloud Hopper; https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html

Carbon Black; Carbon Black Threat Research Dissects Red Leaves Malware, Which Leverages DLL Side Loading; https://www.carbonblack.com/2017/05/09/carbon-black-threat-research-dissects-red-leaves-malware-leverages-dll-side-loading/

CrowdStrike; Two Birds, One STONE PANDA; https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

CrowdStrike; You Have an Adversary Problem; https://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem/

FireEye; APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat; https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

FireEye; APT10 Targeting Japanese Corporations Using Updated TTPs; https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

Japan Computer Emergency Response Team; ChChes – Malware that Communicates with C&C Servers Using Cookie Headers; https://blogs.jpcert.or.jp/en/2017/02/chches-malware--93d6.html

Japan Computer Emergency Response Team; RedLeaves – Malware Based on Open Source RAT; https://blogs.jpcert.or.jp/en/2017/04/redleaves--malware-based-on-open-source-rat.html

LAC; Confirm new attack with APT attacker group menuPass (APT10) [translated]; https://www.lac.co.jp/lacwatch/people/20180521_001638.html

LAC; Relationship between attacker group menuPass and malware "Poison Ivy, PlugX, ChChes" [translated]; https://www.lac.co.jp/lacwatch/people/20170223_001224.html

MITRE; menuPass; https://attack.mitre.org/groups/G0045

NCC Group; Red Leaves implant – overview; https://github.com/nccgroup/Cyber-Defence/blob/master/Technical%20Notes/Red%20Leaves%20technical%20note%20v1.0.pdf

Palo Alto Networks; menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organization; https://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/

PricewaterhouseCoopers & BAE Systems; Operation Cloud Hopper; https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

Trend Micro; ChessMaster Adds Updated Tools to its Arsenal; https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-adds-updated-tools-to-its-arsenal/

Trend Micro; ChessMaster Makes its Move: A Look into the Campaign's Cyberespionage Arsenal; https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/

U.S. Department of Homeland Security; IR-ALERT-MED-17-093-01C, Intrusions Affecting Multiple Victims Across Multiple Sectors; https://www.us-cert.gov/sites/default/publications/IR-ALLERT-MED-17-093-01C-Intrusions_Affecting_Multiple_Victims_Across_Multiple_Sectors.pdf

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.