AWARENESS BRIEFING:
CHINESE CYBER ACTIVITY TARGETING MANAGED SERVICE PROVIDERS
Disclaimer

This report is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise. This document is marked TLP:WHITE. Subject to standard copyright rules. TLP:WHITE information may be distributed without restriction. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.
Welcome and Introductions

Laura Carlson
Stakeholder Engagement Division
Introductory Remarks

Christopher C. Krebs
Director, Cybersecurity and Infrastructure Security Agency
The Nation’s Risk Advisors

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure.
Cybersecurity and Infrastructure Security Agency (CISA)

VISION
A Nation with secure and resilient critical infrastructure that ensures our security, economic prosperity, and way of life.

MISSION
Strengthen the Nation's cyber and physical infrastructure by managing and reducing systemic and catastrophic risk in partnership with the private sector, collaboration with the public sector, and protection of federal government networks.
Our objective with this webinar

Enable you to identify and reduce your exposure to this threat

Underlying message

You can outsource your operations, but you cannot outsource your risk
Target Audience

Managed Service Providers (MSP)

Clients
Housekeeping

• Submit questions and feedback in the Questions box.

• Troubleshooting: Chat with support staff in the Technical Support box.

Please complete the short survey following the webinar.
We appreciate your feedback.
Agenda

- Threat Overview
- Mitigation & Detection
- Q&A
- CISA Offerings
THREAT OVERVIEW
Cyber is the top threat to national security.
China wants what we have

10 sectors

- Robotics and automated machine tools
- Biotechnology
- Next generation information technology
- Aircraft and aircraft components
- Advanced rail equipment
- Agricultural machinery and equipment
- Maritime vessels and marine engineering equipment
- Clean energy vehicles
- New materials
- Electrical generation and transmission equipment

CREDIT: DOJ, Statement of John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice before the Committee on the Judiciary, United States Senate for a hearing on China’s Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses presented on December 12, 2018
China needs cyber espionage

CREDIT: Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community; Daniel R. Coats, Director of National Intelligence, Senate Select Committee on Intelligence; 29 January 2019
Threat Actor: APT 10

Background

- Affiliated with the Ministry of State Security (December 2018 indictment)
- Active since at least 2006
- Becoming increasingly sophisticated and capable

Intent

- Most likely to support commercial and economic espionage
  - Made in China 2025, Five Year Plan
- Could also target PII
- Targets of opportunity
Campaign: CLOUD HOPPER

MSPs as Targets

• Provide unique opportunities for access and collection against large numbers of targets

• Fits a pattern of threat actors increasingly targeting supply chains and trusted relationships

CLOUD HOPPER

• Begins in 2014, picks up in 2016, on-going through 2018 despite public disclosure in 2017

• Targets MSPs and MSP customers on every continent targeted (finance and banking, telecommunications, biotechnology, consulting, automotive...)
Campaign: CLOUD HOPPER

TTPs:

• Initial compromise may be phishing or spearphishing
• Use of common and custom malware (PlugX, RedLeaves, QuasarRAT)
• Living-off-the-Land, stolen credentials, lateral movement
• Encryption of exfiltrated data from target through MSP networks
• Appears to adjust to public disclosure
Key Takeaways

1. This is a serious actor with resources and they require a firm resolve by the defenders.

2. This actor sweeps up collateral targets of opportunity, in addition to their primary targets of interest.

3. This actor lives off the land, and they may use commonplace tools found in your network environments and turn them against you.
MITIGATION & DETECTION
Mitigation Strategies for Managed Service Provider (MSP) Customers

General Mitigation Guidance

Manage Supply Chain Risks
- Understand the supply chain risks associated with their MSP to include determining network security expectations
- Manage risk equally across their security, legal, and procurement groups.

Manage Architecture Risks
- Review and verify all connections between customer systems, service provider systems, and other client enclaves
- Restrict Virtual Private Network (VPN) traffic to and from MSP using a dedicated VPN connection
General Mitigation Guidance

Mitigation Strategies for Managed Service Provider (MSP) Customers

Implement Strong Operational Controls

• Create baseline for system and network behavior; continuously monitor network devices SIEM appliance alerts
• Regularly update software and operating systems

Manage Authentication, Authorization, and Accounting Procedures

• Adhere to best practices for password and permission management
• Ensure MSP accounts are not assigned to administrator groups and restrict those accounts to only systems they manage
General Mitigation Guidance

Mitigation Strategies for Managed Service Providers (MSP)

- Ensure they have fully implemented all mitigation actions available to protect against this threat.
- Apply the principle of least privilege to their environment.
- Implement robust network and host-based monitoring solutions.
- Ensure that log information is aggregated and correlated to enable maximum detection capabilities.
- Work with their customers to ensure hosted infrastructure is monitored and maintained.
Specific Mitigation Guidance

Mitigation Strategies for known TTPs

- DLL Search Order Hijacking
  - Disallow loading of remote DLLs

- Enable Safe DLL Search Mode
  - Forces the use of restricted directories

- Implement tools for detecting search order hijacking opportunities

- Utilize application whitelisting to block unknown DLLs
Monitoring for DLL Search Order Hijacking

- Monitor file system for created, moved, renamed DLL’s
- Changes in system DLL’s not associated with updates/patches are suspicious
- Monitor DLL’s loaded by processes (legitimate names, abnormal path)
Logging

Enable and audit advanced PowerShell logging

User account activity (focus on administrator level accounts)
Network Activity

Monitor processes for outbound network activity (against baseline)

Monitor connections to MSP infrastructure
Key Takeaways

1. Good credentials management goes a long way.

2. Foreclosing the doors this actor uses to move, hide, and attack can be done through good cyber hygiene.

3. Recognizing normal versus abnormal system and network behavior is still the longest yard to make.
Q&A

How do we learn about these types of malicious activities?
Q&A

What are the benefits of reporting this information?
CISA Offerings

CISA offers a collection of resources and tools to support identification of and defense against Chinese malicious activity

- A comprehensive list of mitigation strategies for IT service providers can be found at [https://www.us-cert.gov/china](https://www.us-cert.gov/china)

Organizations that determine their risk to be elevated should conduct a dedicated investigation to identify any Chinese related activity

- Contact CISA NCCIC
  ncciccustomerservice@hq.dhs.gov
  888-282-0870

- Report unauthorized network access to your local FBI Cyber Division
  cywatch@fbi.gov
  855-292-3937
We
Need
You

Engage with us, share with us.
One entity’s detection is another’s prevention.

We’re all in this together.

DEFEND TODAY. SECURE TOMORROW.
For more information:
cisa.gov

For media inquiries, contact
nppdmedia@hq.dhs.gov

Report incidents
Email:
nccicccustomerservice@hq.dhs.gov
Phone: 1-888-282-0870