


NETWITNESS 
FIRSTWATCH

INTSUM REPORT

5 – 17 July 2024



BIWEEKLY INTELLIGENCE SUMMARIES (INTSUM) WILL REPORT ON THE MOST NOTEWORTHY RANSOMWARE ATTACKS, WIDELY EXPLOITED VULNERABILITIES AND THE LATEST IN DATA PRIVACY AND SECURITY POLICY NEWS TO PROVIDE A VALUABLE SNAPSHOT AND BRIEF SYNOPSIS OF THE CURRENT THREAT LANDSCAPE



New APT group CloudSorcerer Uses Cloud Services to Target Russian Government Entities

A new group of hackers, CloudSorcerer, has been discovered targeting Russian government agencies. These hackers use special software to secretly gather and send out information through popular cloud services like Dropbox and Microsoft Graph. Their attacks are somewhat similar to previous ones known as CloudWizard, but CloudSorcerer uses its own unique methods and tools. To combat such threats, it's crucial to adopt proactive cybersecurity measures, empowering us to stay prepared and protected.

They begin their attacks by communicating through platforms like GitHub and Mail.ru and then use services such as Yandex Cloud, Microsoft Graph, and Dropbox to collect data and carry out commands. This group is smart in how it changes its tactics depending on which program it's working through.

Although it's unclear who is behind CloudSorcerer, there's speculation they may be from a Western country, with the U.S. being a likely candidate. This situation highlights that cyber threats are a worldwide problem, affecting not just Europe or North America. To protect against such threats, organizations need to monitor incoming and outgoing data traffic, blocking unnecessary access to potentially risky web services.

NetWitness Takeaways:

NetWitness SIEM Windows parser efficiently parses all Windows system, application, and security logs from all events.



New APT group CloudSorcerer Uses Cloud Services to Target Russian Government Entities

NetWitness Takeaways (cont.):

Hunting Queries:

- **Suspicious Cloud API Interactions:**

```
device.type = 'windows' && category = 'process creation' &&  
process = 'c:\\windows\\system32\\msiexe.exe' && param  
contains 'api.github.com', 'api.dropbox.com', 'graph.microsoft.com',  
'cloud-api.yandex.net'
```

- **Uncommon Process requests to Cloud APIs:**

```
device.type = 'nwendpoint' && category = 'console event' &&  
action = 'createprocess' && filename.src =  
'c:\\windows\\system32\\powershell.exe' && param.src contains  
'invoke-webrequest', 'iwr' && param.src contains 'api.github.com',  
'api.dropbox.com', 'graph.microsoft.com', 'cloud-api.yandex.net'
```

- **Malicious CloudSorcerer Command Patterns:**

```
device.type = 'nwendpoint' && category = 'console event' &&  
action = 'createprocess' && filename.src =  
'c:\\windows\\system32\\powershell.exe' && param.src contains  
'invoke-webrequest', 'iwr' && param.src contains 'api.github.com',  
'api.dropbox.com', 'graph.microsoft.com', 'cloud-api.yandex.net'
```

MITRE ATT&CK Techniques:

- T1059: Command-Line Interface
- T1064: Scripting
- T1027: Obfuscated Files or Information
- T1538: Cloud Service Discovery
- T1530: Data from Cloud Storage
- T1485: Data Destruction



Operation Morpheus Targets Illegal Cobalt Strike Servers

Recently, a joint law enforcement operation, Operation Morpheus, led to the takedown of hundreds of unlicensed Cobalt Strike servers. This significant action, coordinated by Europol and led by the UK's National Crime Agency (NCA), was the result of two-and-a-half years of collaborative work between international law enforcement agencies (the FBI, Australian Federal Police, Royal Canadian Mounted Police, German Federal Criminal Police Office, Netherlands National Police and the Polish Central Cybercrime Bureau) and several key private industry partners (BAE Systems Digital Intelligence, Trellix, Shadowserver, Spamhaus and Abuse CH), whose contributions were instrumental in the success of the operation.

Released by Fortra in 2012, Cobalt Strike is a legitimate penetration testing and red teaming software. The tool simplifies several post-exploitation actions an attacker may take in victim environments, including establishing persistence, setting up command-and-control communications, information gathering/exfiltration, and secondary payload retrieval. Due to its ease of use, illegal or "cracked" versions of Cobalt Strike are abused by numerous cyber adversaries, including nation-state actors APT 29 and APT32 and financially motivated groups FIN6 and FIN7.

Operation Morpheus occurred over a single week at the end of June. During the first part of the action, law enforcement identified known attacker IP addresses and domains associated with illegal Cobalt Strike software. In the second stage, the joint task force sent "abuse notifications" to ISPs informing them of any discovered unlicensed versions of Cobalt Strike. According to NCA, "Action was taken against 690 individual instances of malicious Cobalt Strike software located at 129 internet service providers in 27 countries. By the end of the week, 593 of these addresses had been taken down."



Operation Morpheus Targets Illegal Cobalt Strike Servers (cont.)

Information sharing between private industry partners and law enforcement was crucial to the operation's success. Using the Malware Information Sharing Platform (MISP), the joint task force shared over "730 pieces of threat intelligence containing almost 1.2 million indicators of compromise."

NetWitness Takeaways:

- Google Cloud Threat Intelligence [released several YARA rules](#) to detect the behavioral characteristics of Cobalt Strike. NetWitness Endpoint customers can deploy these rules to monitor Cobalt Strike activity further.
- For additional NetWitness coverage of Cobalt Strike, please check out the following NetWitness Community blog post:
 - [Detecting C&C Malleable Profiles](#)
- The following Application Rules, currently available on NetWitness Live, can help in detection of Cobalt Strike within customer networks:
 - NetWitness Endpoint
 - Cobalt Strike Getsystem Service Detected
 - Cobalt Strike Service Installations in Registry
 - SearchProtocolHost.exe Launched Without Arguments
 - Suspicious SearchProtocolHost.exe Network Traffic



Operation Morpheus Targets Illegal Cobalt Strike Servers (cont.)

MITRE ATT&CK Techniques:

- T1059.001: Command-Line Interface
- T1027: Obfuscated Files or Information
- T1089: Disabling Security Tools
- T1087: Account Discovery
- T1018: Remote System Discovery
- T1003.003: OS Credential Dumping: LSASS Memory
- T1021.002: Remote Services: SMB/Windows Admin Shares
- T1021.001: Remote Services: Remote Desktop Protocol
- T1113: Screen Capture
- T1105: Remote File Copy
- T1041: Exfiltration Over Command and Control Channel



Emerging Phishing Campaign Targets Latin American Industries with Poco RAT

A new phishing campaign has emerged, targeting Spanish-speaking victims in Latin America, predominantly affecting the mining and manufacturing sectors. This campaign delivers a remote access trojan (RAT) known as Poco RAT, which Cofense discovered in early 2024. The malware is propagated through finance-themed phishing emails written in Spanish. These emails contain malicious links to Google Drive-hosted 7zip archives or embedded links in HTML and PDF files.

Poco RAT, utilizing the POCO C++ libraries, is a stealthy, custom-built malware designed to evade detection. It focuses on anti-analysis, communication with its command-and-control (C2) server, and downloading additional malware. The phishing emails follow a consistent pattern: finance-themed subjects and bodies in Spanish, with direct Google Drive URLs or embedded links. These tactics enable the malware to bypass secure email gateways (SEGs) by appearing legitimate, underscoring the need for heightened vigilance.

Upon execution, Poco RAT establishes persistence, launches the legitimate process `grpconv.exe`, and connects to its C2 server at `94[.]131.119.126`, responding only to Latin American geolocated requests. The malware is written in Delphi, often packed with UPX, and includes extensive metadata to evade detection further. To mitigate the threat, it is recommended to treat Google Drive links as potentially malicious, blocking traffic to the known C2 address, and monitoring for unusual executions of `grpconv.exe` to mitigate the threat.



Emerging Phishing Campaign Targets Latin American Industries with Poco RAT (cont.)

NetWitness Takeaways:

- Implement robust email spam detection mechanisms to filter out emails that exhibit typical phishing characteristics.
- Train employees to recognize phishing emails, suspicious links, and requests for sensitive information.

Hunting Queries:

- `device.type = 'nwendpoint' && category = 'network event' && direction = 'outbound' && port.dst = '6541', '6542', '6543' && ip.dst = '94.131.119.126'`
- `device.type = 'nwendpoint' && category = 'process event' && filename.src = 'powershell.exe' && filename.dst = 'grpconv.exe'`

MITRE ATT&CK Techniques:

- T1566.001: Spearphishing Link
- T1566.002: Spearphishing Attachment
- T1056.001: Input Capture: Keylogging
- T1056.003: Input Capture: Credential API Hooking
- T1134.001: Access Token Manipulation: Token Impersonation/Theft
- T1115: Clipboard Data
- T1204.002: User Execution: Malicious File
- T1048: Exfiltration Over Alternative Protocol

