


NETWITNESS 
FIRSTWATCH

INTSUM REPORT

18 – 31 July 2024



WEEKLY 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

MIRRORFACE Digs in for the Long-term

MirrorFace represents a state-sponsored initiative originating from China that has been active for at least five years. Comparable to other campaigns like LiberalFace, its activities are primarily directed against India, Japan, and Taiwan, with umbrella operations identified in Thailand and the US. The principal focus, however, remains on Japanese political circles. The campaign's modus operandi is uniquely tailored to exploit Japanese technological environments, notably demonstrated through its manipulation of the Japan-specific JustSystems word processor.

Recent analysis, particularly in early 2024 by cybersecurity oversight teams from ESET and Trend, highlighted through publications by JPCERT, emphasizes the evolving tactics of the MirrorFace campaign. The intrusion starts with the remote exploitation of vulnerable public-facing web applications. The attackers utilize sideloading techniques facilitated by MSBuild.exe LOLbin processes, engaging a .dat file through a build XML file identified as NOOPLDR, to execute malicious code within the targeted network. The campaign strategically employs Cobalt Strike Beacons, identifiable by a specific watermark, to enhance its penetration and control within the infrastructure.

Commands including “csvde -f all.csv -u”, “nltest /domain_trust”, and “quser” distinguish the campaign's sophisticated efforts to navigate and exploit the network environment. Furthermore, the deployment of a payload named MirrorStealer signifies a calculated move to harvest an array of credentials, targeting not only web browsers and email clients such as Chrome, Firefox, Edge, Internet Explorer, Thunderbird, Outlook, Live Mail, and Becky! Internet Mail, but also areas secured by Group Policy Preferences (GPPs) and MS-SQL Server credentials.



MIRRORFACE Digs in for the Long-term (cont.)

To achieve long-term access and data exfiltration, the operatives meticulously manage Domain Admin credentials via Remote Desktop Protocol, establishing persistence through scheduled tasks and packaging outbound data with make cab for transmission via RDP client. The operation concludes with clearing WinEvt logs to obscure their activity trails. MirrorFace, in its intricate execution and tailored targets, exemplifies the evolving landscape of state-sponsored cyber espionage, emphasizing a high level of sophistication and a clear focus on long-term infiltration and intelligence gathering.

NetWitness Takeaways:

IOCs:

0d59734bdb0e6f4fe6a44312a2d55145e98b00f75a148394b2e4b86436c32f4c
43349c97b59d8ba8e1147f911797220b1b7b87609fe4aaa7f1dbacc2c27b361d
572f6b98cc133b2d0c8a4fd8ff9d14ae36cdaa119086a5d56079354e49d2a7ce
5e7cd0461817b390cf05a7c874e017e9f44eef41e053da99b479a4dfa3a04512
7a7e7e0d817042e54129697947dfb423b607692f4457163b5c62ffea69a8108d
93af6afb47f4c42bc0da3eedc6ecb9054134f4a47ef0add0d285404984011072
9590646b32fec3aafd6c648f69ca9857fb4be2adfabf3bc321c8cd25ba7b83
b07c7dfb3617cd40edc1ab309a68489a3aa4aa1e8fd486d047c155c952dc509e
bcd34d436cbac235b56ee5b7273baed62bf385ee13721c7fdcf00af9ed63997
45[.]66.217.106
45[.]76.222.130
45[.]77.12.212
45[.]77.183.161
64[.]176.214.51
89[.]233.109.69
95[.]85.91.15
108[.]160.130.45
168[.]100.8.103
207[.]148.90.45
207[.]148.97.235
207[.]148.103.42



MIRRORFACE Digs in for the Long-term (cont.)

NetWitness Takeaways (cont.):

YARA Rule

```
rule Trojan_NOOPLDR_xml
{
meta:
Author = "Trend Micro"
Created_Time = "2024-01-26"
strings:
$s1 = "<Code Type=\"Class\" Language=\"cs\"><![CDATA[using "
$s2 = "Software\\\\"Microsoft\\\\"SQMClient"
$s3 = ".GetValue(\"MachineId\").ToString()"
$s4 = "SHA384.Create();"
$s5 = "new byte[32];Array.Copy("
$s6 = "new byte[16];Array.Copy("
condition:
all of them
}
```

MITRE ATT&CK Techniques:

- T1133 - External Remote Services
- T1053.005 - Scheduled Task
- T1543.003 - Windows Service
- T1134 - Access Token Manipulation
- T1055 - Process Injection
- T1070.004 - File Deletion
- T1070.001 - Clear Windows Event Logs
- T1070.006 - Timestamp
- T1127.001 - MSBuild
- T1562.001 - Disable or Modify Tools
- T1021.002 - SMB/Windows Admin Shares
- T1568.002 - Domain Generation Algorithms
- T1560.001 - Archive via Utility



MuddyWater Adopts BugSleep Backdoor in Evolving Cyber-Espionage Tactics

The Iranian cyber-espionage group MuddyWater, affiliated with the Ministry of Intelligence and Security (MOIS), has recently transitioned from using legitimate remote-management software to deploying a custom-made backdoor implant named BugSleep (also known as MuddyRot). This shift was observed in recent campaigns targeting countries including Israel, Turkey, Azerbaijan, Jordan, Saudi Arabia, and Portugal. Previously, MuddyWater utilized tools like SimpleHelp and Atera to maintain access to compromised systems through spear-phishing emails. However, the latest campaigns distribute malicious PDF files with embedded links, leading to files hosted on the secure file-sharing program called Egnyte, which installs BugSleep.

BugSleep, identified in May 2024, is still under development and includes anti-analysis techniques such as delaying execution to evade sandbox detection. The backdoor, developed in C, allows attackers to download/upload files, launch a reverse shell, and establish persistence via a raw TCP socket on port 443. Despite its advanced capabilities, BugSleep has several bugs and encryption issues, suggesting ongoing development. The shift from Remote Management Tools (RMM) tools such as Atera Agent, RemoteUtilities, ScreenConnect, SimpleHelp, or Syncro to a custom implant is likely due to increased monitoring of RMM tools by security vendors.

MuddyWater, active since at least 2017, has targeted a wide range of sectors, including government, telecommunications, and critical infrastructure, primarily in the Middle East. The group's phishing campaigns have evolved to simpler lures focusing on generic themes like webinars and online courses, allowing for higher volume attacks.



MuddyWater Adopts BugSleep Backdoor in Evolving Cyber-Espionage Tactics (cont.)

These campaigns mainly target organizations in Israel and Saudi Arabia but extend to India, Jordan, Portugal, Turkey, and Azerbaijan. MuddyWater's persistent and aggressive phishing strategies and the development of BugSleep underscore their significant threat to cybersecurity in the Middle East and beyond.

NetWitness Takeaways:

- Preventing attacks from APT groups like MuddyWater requires a comprehensive approach involving user training and proactive threat detection.
- Educate employees on phishing risks and how to handle suspicious emails and attachments.
- Apply the principle of least privilege and enforce Multi-Factor Authentication (MFA) for critical accounts.
- For additional NetWitness coverage of MuddyWater APT, please check out the following NetWitness Community blog post:
 - <https://community.netwitness.com/t5/netwitness-community-blog/detecting-a-muddywater-apt-using-the-rsa-netwitness-platform/ba-p/521145>
- The following NetWitness Endpoint Application Rules, currently available in NetWitness Live, can help identify TTPs associated with MuddyWater APT:
 - Runs Powershell Downloading Content
 - Runs Powershell Decoding Base64 String
 - Runs Credential Dumping Tools





MuddyWater Adopts BugSleep Backdoor in Evolving Cyber-Espionage Tactics (cont.)

NetWitness Takeaways (cont.):

MITRE ATT&CK Techniques:

- T1566.001 - Phishing: Spearphishing Attachment
- T1566.002 - Phishing: Spearphishing Link
- T1204.002 - User Execution: Malicious File
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1068 - Exploitation for Privilege Escalation
- T1027 - Obfuscated Files or Information
- T1003 - Credential Dumping
- T1041 - Exfiltration Over C2 Channel



Global Industrial Control Systems at Risk: FrostyGoop Malware Targets Modbus Protocol

The investigation into the January 2024 cyberattack in Lviv uncovered that the attackers took advantage of a still unknown vulnerability in an Internet-exposed Mikrotik router to gain access to Lvivteploenergo's network on April 17, 2023. Three days later, they installed a web shell to maintain access. They accessed the compromised network in November and December to steal user credentials from the Security Account Manager (SAM) registry hive.

Threat actors can exploit the open port 502 to initiate an attack using TCP/IP messages. A search on Shodan.io revealed 90 exposed Modbus devices in the United States alone, indicating that hackers can rely on this protocol to target industrial control systems (ICS). Modbus, a client/server communication protocol initially designed for Modicon PLCs in 1979, is widely used in various ICS/OT devices due to its hardware agnostic nature and popularity for communication between PLCs, distributed control systems, controllers, sensors, actuators, field devices, and interfaces.

Initially, the attackers accessed the district energy company's network assets using L2TP connections from IP addresses based in Moscow. Due to the lack of proper network segmentation in Lvivteploenergo's network, including the compromised MikroTik router, four management servers, and the district's heating system controllers, the attackers were able to exploit hardcoded network routes and take control of the district's heating system controllers. They later downgraded the controllers' firmware to versions without monitoring capabilities to avoid detection.



Global Industrial Control Systems at Risk: FrostyGoop Malware Targets Modbus Protocol (cont.)

Dragos issued a warning about the malware's potential to disrupt all industrial sectors by interacting with both legacy and modern systems. They emphasized the widespread use of the Modbus protocol in industrial environments. They recommended that industrial organizations adopt the SANS 5 Critical Controls for World-Class OT Cybersecurity, which includes ICS incident response, defensible architecture, ICS network visibility and monitoring, secure remote access, and risk-based vulnerability management.

NetWitness Takeaways:

- Organizations with critical infrastructure sectors must prioritize assessing and protecting their ICS networks by restricting access to Modbus devices and conducting thorough network assessments to ensure they are not exposed to the Internet.
- Netwitness offers a Modbus lua parser for greater visibility over the Modbus protocol. Enable the parser for efficient detection.

IOCs:

5d2e4fd08f81e3b2eb2f3eaae16eb32ae02e760afc36fa17f4649322f6da53fb
a63ba88ad869085f1625729708ba65e87f5b37d7be9153b3db1a1b0e3fed309c





Global Industrial Control Systems at Risk: FrostyGoop Malware Targets Modbus Protocol (cont.)

NetWitness Takeaways (cont.):

YARA Rule:

```
rule Mal_Hacktool_Win64_Bustleberm
{
meta:
  name = "BUSTLEBERM ICS Hacktool"
  author = "Nozomi Networks Labs"
  description = "Detects the BUSTLEBERM ICS Hacktool (also known as FrostyGoop)"
  date = "2024-07-24"
  tlp = "clear"
  x_threat_name = "BUSTLEBERM"
x_mitre_technique = "T1007, T1012, T1033, T1112, T1543, T0869, T0855"
  reference = "https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-
Malware-Intel-Brief-0724 .pdf"
  hash1 = "5d2e4fd08f81e3b2eb2f3eaae16eb32ae02e760afc36fa17f4649322f6da53fb"
  hash2 =
"a63ba88ad869085f1625729708ba65e87f5b37d7be9153b3db1a1b0e3fed309c"
strings:
  $go = "Go build ID:" ascii fullword
  $modbus_1 = "github.com/rolfl/modbus" ascii fullword
  $modbus_2 = "\x00main.MbConfig.writeMultiple\x00" ascii
  $rtn_1 = "\x00main.TaskList.executeCommand\x00" ascii
  $rtn_2 = "\x00main.TaskList.getTaskIpList\x00" ascii
  $rtn_3 = "\x00main.TaskList.getIpList\x00" ascii
  $rtn_4 = "\x00main.TargetList.getTargetIpList\x00" ascii
condition:
  uint16(0) == 0x5a4d and
  filesize <= 10MB and
  $go and
  any of ($modbus_*) and
  2 of ($rtn_*)
}
```





FIRSTWATCH

Global Industrial Control Systems at Risk: FrostyGoop Malware Targets Modbus Protocol (cont.)

NetWitness Takeaways (cont.):

MITRE ATT&CK Techniques:

- T0855 - Unauthorized Command Message
- T0869 - Standard Application Layer Protocol
- T1007 - System Service Discovery
- T1012 - Query Registry
- T1033 - System Owner/User Discovery
- T1112 - Modify Registry
- T1543 - Create or Modify System Process

