SECURITY ADVISORY

CYBER STASH

August, 2024

# CMoon USB Worm Data Theft Attack

## Context

A newly identified USB worm, designated "CMoon," has emerged with a specific focus on Russian individuals and organizations. This sophisticated malware is engineered for data exfiltration, with the primary goal of pilfering sensitive information from compromised systems. The worm exploits USB drives as its attack vector, rendering it particularly formidable in environments where shared or transient storage media are prevalent. The appearance of CMoon has provoked substantial concern due to its potential ramifications for both governmental and private sector entities within Russia.

The modus operandi of this attack involves deceiving users into interacting with seemingly benign links to regulatory documents—such as .docx, .xlsx, .rtf, and .pdf files—hosted on a company's website. These links have been clandestinely altered by threat actors, replacing the genuine documents with malicious executables. The payloads are distributed through self-extracting archives, which contain both the ostensibly legitimate document and the malevolent CMoon malware. Upon downloading and opening these archives, users inadvertently execute the CMoon payload, which then establishes a backdoor or engages in other nefarious activities, thereby granting the attackers control over the affected systems. This technique capitalizes on the users' inherent trust in the legitimacy of regulatory documents and the company's website to facilitate the infection chain.

## Mitigation

Defending against the CMoon attack requires immediate and proactive measures:

**Deploy Advanced Endpoint Protection:** Utilize endpoint protection software with heuristic and behavior-based detection to identify and neutralize CMoon's evasive tactics and malicious activities.

**Restrict USB Access and Monitor Network Traffic:** Limit USB drive usage through access controls and actively monitor network traffic for unusual patterns or encrypted communication indicative of CMoon's command-and-control operations.

**Blocking Network Traffic:** Implement proactive network traffic blocking measures, including the restriction of suspicious IPs, domains, and connections from high-risk Autonomous System Numbers, Top-Level Domains, and countries.

## Technical Details

CMoon is a sophisticated .NET-based worm distinguished by its robust data theft and remote control capabilities. Upon infiltrating a system, CMoon initially scans for antivirus software; if none is detected, it installs itself in the %LocalAppData%\.dat directory and creates a startup shortcut in %AppData%\Microsoft\Windows\Start Menu\Programs\Startup.lnk.

The worm then obfuscates its presence by altering the creation and modification timestamps of its files to appear as if they were generated on May 22, 2013.

A notable feature of CMoon is its ability to monitor and exploit connected USB drives. It pilfers files from these drives and propagates itself to other systems by substituting legitimate files with shortcuts leading to the malware, while deliberately avoiding modification of files with .lnk and .exe extensions, as well as those within directories containing .intelligence and .usb substrings.

CMoon can receive directives from a remote server to execute a range of operations, including the downloading and execution of additional malicious payloads, capturing screenshots, launching distributed denial-of-service (DDoS) attacks, and gathering intelligence about local network resources. Prior to establishing a connection with its command server, CMoon verifies internet connectivity by querying a known server. Communications with the command server occur over a TCP connection, with outgoing packets prefixed by "CMOON$" and encrypted using an RC4 key, carrying varied data such as system information, Wi-Fi profiles, and screenshots.

The worm targets an extensive array of applications to exfiltrate sensitive information, including browsers, cryptocurrency wallets, messaging clients, SSH and FTP clients, video recording software, authenticators, remote access tools, and VPN clients.

## Tactics, Techniques and Procedures

The notable TTPs related to the CMoon are:

**T1195.00 - Initial Access:** The worm gains access through infected USB drives, exploiting user interaction for execution.

**T1059 - Execution:** The worm uses scripts and command-line interfaces to execute its payload once the USB is inserted.

**T1547 - Persistence:** CMoon establishes persistence by modifying registry keys and utilizing startup folders.

**T1055 - Privilege Escalation:** The worm attempts to escalate privileges to gain full control over the system.

**T1119 - Collection:** The worm systematically collects data by searching for files with specific extensions.

**T1041 Exfiltration:** Collected data is exfiltrated via network channels, possibly using encrypted communications.

## Cyber Threat Intelligence

The CMoon worm appears to be a targeted attack with a primary focus on Russian entities. The underlying motivation is likely espionage, aiming to exfiltrate sensitive information from both governmental and private sector networks. The worm's use of USB drives as a propagation vector suggests that the attackers may be exploiting environments with restricted or closely monitored internet access, such as air-gapped systems.

Given the ongoing conflict between Russia and Ukraine, it is also plausible that the attacker behind CMoon could be linked to Ukrainian state actors or affiliated entities. The malware's targeted nature and sophisticated capabilities might reflect a strategic effort to counteract Russian cyber operations or gather intelligence on Russian activities. This scenario would align with broader geopolitical cyber strategies, where both sides leverage advanced malware to gain tactical advantages and disrupt adversaries. Such a possibility underscores the complex dynamics of cyber warfare in the current conflict.

CyberStash anticipates that Russian state actors may reverse engineer CMoon and modify it for use against Western targets. This anticipated adaptation and deployment of CMoon in retaliation could pose substantial cybersecurity risks to Western nations, highlighting the broader and more significant implications of this malware's emergence.

# References

## Related Yara Rule:

```
rule Detect_CMoom_Worm
{
   meta:
      description = "Detects CMoon worm based on known characteristics"
      author = "CyberStash"
      date = "2024-08-15"
      reference = "Custom YARA rule for CMoon detection"

   strings:
      $file_marker = "CMOON$" // Unique packet prefix
      $rc4_key_pattern = { 00 00 00 00 00 00 00 00 } // Placeholder for RC4 key pattern
      $dat_file_path = "%LocalAppData%\\.dat" // File path indicator
      $startup_shortcut = "%AppData%\\Microsoft\\Windows\\Start
Menu\\Programs\\Startup.lnk" // Startup shortcut path
      $modification_date = "2013-05-22" // Date manipulation pattern

   condition:
      // Detects the presence of CMoon based on unique patterns
      ($file_marker in (filesize < 10MB) and $rc4_key_pattern in (filesize < 10MB)) or
      ($dat_file_path in (filesize < 10MB) and $startup_shortcut in (filesize < 10MB)) or
      (filename contains ".dat" and filesize < 1MB) and
      (filetime >= 2013-05-22T00:00:00 and filetime < 2013-05-23T00:00:00)
}
```

# References

## IOCs:

| Type | Indicators |
|---|---|
| **Domains** | vqdn[.]net, mwgq[.]net, wak[.]rocks, o7car[.]com, 6t[.]nz, fcgz[.]net, d0[.]wf, e0[.]wf, c4z[.]pl, 5g7[.]at, 5ap[.]nl, 4aw[.]ro, 0j[.]wf, f0[.]tel, h0[.]pm, y0[.]pm, 5qy[.]ro, g3[.]rs, 5qe8[.]com, 4j[.]pm, m0[.]yt, zk4[.]me |
| **IP Addresses** | 59.15.11[.]49, 82.124.243[.]57, 114.32.120[.]11, 203.186.28[.]189, 70.124.238[.]72, 73.6.9[.]83, 93.185.167[.]95 |
| **MD5** | 132404f2b1c1f5a4d76bd38d1402bdfa |

## Public Intelligence:

- https://www.bleepingcomputer.com/news/security/new-cmoon-usb-worm-targets-russians-in-data-theft-attacks/
- https://cybersecuritynews.com/new-cmoon-worm-attacking/
- https://securelist.ru/how-the-cmoon-worm-collects-data/109988/
- https://cyber.vumetric.com/security-news/2024/08/07/new-cmoon-usb-worm-targets-russians-in-data-theft-attacks/