Malware campaign abuses ‘fertile ground’ of Microsoft log files, an unexplored frontier for infosec researchers

-security) › (https://gurucul.com/news/malware-hides-in-clfs-to-evade-detection)

By Admin September 13, 2021

Bradley Barth | Scmagazine.com »

Cybercriminals are hiding second-stage malware payloads in Common Log File System (CLFS) files as a means to avoid detection, taking advantage of a new storage mechanism whose inner workings are not well known by security researchers.

FireEye’s Mandiant Advanced Practices team reported their discovery of the scheme, which involves a new malware called Privatelog and its corresponding installer, Stashlog. These two malwares hide malicious code in registry transaction files by abusing CLFS, which is a Microsoft log framework that provides applications with API functions to enable the creation, storage and viewing of log data.

The adversaries behind this campaign are capitalizing on the fact that the CLFS master and container file formats are “not widely used or documented,” and “there are no available tools that can parse CLFS log files,” according to a recent FireEye blog post (https://www.fireeye.com/blog/threat-research/2021/09/unknown-actor-using-clfs-log-files-for-stealth.html).

“No one in security really knows the exact structure of these files except Microsoft, so this makes it a dangerous hiding place to deliver malware while avoiding detection,” said Matthew Dunwoody, senior principal researcher, advanced practices at Mandiant, in an interview with SC Media.

The blog post said the Privatelog campaign works similarly to malware “which may rely, for example, on the Windows Registry or NTFS Extended Attributes to hide their data, which also provide locations to store and retrieve binary data with the Windows API.” Dunwoody also cited the Common Information Model (CIM) repository as another abused storage location, “but this one is new in our experience.”

“If defenders aren’t aware of this technique, they may not be able to effectively locate the hidden data or fully respond to the activity. These fileless techniques can also complicate scanning by anti-virus tools, as the storage location may not be scanned, or the storage technique may change the format of the data,” said Dunwoody, warning that attackers in the future will likely find additional storage locations to abuse, “and it will be important that we identify those new locations.”

“This discovery shows that threat actors are always on the lookup for obscure haystacks to hide needles in,” said John Bambenek, threat intelligence advisor at Netenrich. “The problem with any log file is that the amount of data is often too large for any real attempt at manual examination. Often, SIEMs are little more than digital dumpsters to check the compliance ‘centralized logging’ box. As most detection is designed around to find specific ‘badness,’ many analysts overlook non-normal log entries.”

“Log files represent fertile ground for attacking data on systems and networks,” agreed **Saryu Nayyar**, CEO at Gurucul (/). “Few organizations study their log files to better understand their computing environments, so they mostly just sit there. In this case, the CLFS log format doesn’t even have any tools available to be able to read it, so what better a place to store hacker data?”

Mandiant has not spotted any Privatelog attacks in the wild yet, which means that the malware is either still in a development phase, the work of a researcher, or being used sparingly for targeted attacks. But in case this novel attack technique becomes more commonplace, there are at least a few steps user organizations can take to prepare.

For starters, Mandiant recommends static hunting with Yara rules, and also seeking out indicators of compromise in “process”, “imageload” or “filewrite” events of EDR logs.

In the future, it may be possible that someone will develop an automated took to look for CLFS log file tampering and abuse, but first “the format would need to be analyzed and understood before a tool could be built,” said Dunwoody.

“When looking for malware, you need to know where to look for it, and this isn’t an area that the industry looked at because no one knew you could store binary data in CLFS logs,” Dunwoody continued. “Now that we know this is an area that we need to search for potential dangers, we – and likely the rest of the security community – will begin tailoring solutions to address this.”

As for the CLFS framework itself, Dunwoody said that it “is part of Windows and users shouldn’t try to disable it.”

“As this behavior hasn’t been observed in the wild yet, I wouldn’t make any logging infrastructure changes beyond using the hunting indicators given by FireEye yet,” agreed Bambenek. However, “organizations can and should pay attention to SIEM log parsing errors, as this could indicate non-normal information being in the log files that may indicate similar file or data hiding techniques.”

On the other hand, Nayyar recommended a more aggressive strategy. “The easy answer to this type of attack is that if you’re not using the log data, don’t log it. Turn off logging,” said Nayyar. “If you insist on logging, examine the log files on a regular basis to ensure they haven’t been corrupted. Note when data is written into them and keep track of how that data is accessed.”

The Mandiant post also reported that both Privatelog and Stashlog use an obfuscation technique that involves “XOR’ing each byte with a hard-coded byte inline, with no loops,” such that “each string is… encrypted with a unique byte stream. Additionally, the installer Stashlog’s code is shielded with “various control flow obfuscation techniques” designed to trip up static analysis.

External Link: Malware campaign abuses ‘fertile ground’ of Microsoft log files, an unexplored frontier for infosec researchers (https://www.scmagazine.com/analysis/malware/malware-campaign-abuses-fertile-ground-of-microsoft-log-files-an-unexplored-frontier-for-infosec-researchers)

Cybersecurity (https://gurucul.com/tag/cybersecurity) Data Protection (https://gurucul.com/tag/data-protection) Malware Attack (https://gurucul.com/tag/malware-attack)

Related Posts

Products Solutions

Gurucul Analytics-Driven SIEM (/products/gurucul-siem)
Cost Efficient Cloud Native SIEM

Gurucul User & Entity Behavior Analytics (/products/user-entity-behavior-analytics-ueba)
Continuous Anomaly Detection & Remediation

Gurucul XDR (/products/gurucul-xdr)
Augmented Threat Detection & Faster Incident Response

Gurucul Identity Analytics (/products/identity-analytics)
Real-Time Access Control Automation Using Risk & Intelligence

Gurucul Fraud Analytics (/products/fraud-analytics)
Holistic Cross-Channel Fraud Detection & Prevention

Recent Posts

- Marketron Suffers BlackMatter Attack, Shuts Down All svcs. – 5 Experts Comment (https://gurucul.com/news/marketron-suffers-blackmatter-attack-shuts-down-all-svcs)
- MoD Shares Afghanistan Interpreter's Emails & PII (https://gurucul.com/news/mod-shares-afghanistan-interpreters-emails-pii)
- Thousands of sensitive event records potentially leaked via misconfigured EventBuilder app (https://gurucul.com/news/sensitive-event-records-leaked-via-misconfigured-eventbuilder-app)
- TTEC Hit with Ransomware (https://gurucul.com/news/ttec-hit-with-ransomware)
- Securing the Edge in the Supply Chain (https://gurucul.com/news/securing-the-edge-in-the-supply-chain)

SECURITY

- Gurucul Risk Analytics (GRA)
- Gurucul Analytics-Driven SIEM
- Gurucul UEBA
- Gurucul XDR
- Risk-Driven SOAR

Gurucul Security Data Lake

Gurucul ML-Based NTA

Cloud Security Analytics

Insider Threat

Medical Device Discovery & Monitoring

MITRE ATT&CK Analytics

Zero Trust Security

IDENTITY

Identity Analytics

Privileged Access Intelligence

Risky Account Discovery & Cleanup

Risk Based Access Certifications

Risk Based Authentication

Dynamic Access & Role Modeling

SoD Intelligence

FRAUD

- Fraud Analytics
- Account Takeover & Login Fraud
- Anti-Money Laundering
- Call Center Fraud
- Credit Card Fraud
- Insider Fraud
- Mobile Fraud
- Payment Fraud
- Transaction Fraud
- Regulatory Compliance

ABOUT US

- Company
- Contact Us
- Leadership

Board Of Advisors

Blog

Press Releases

News

Careers

Business Continuity

Glossary

(https://www.facebook.com/gurucul) (https://www.linkedin.com/company/gurucul) (https://twitter.com/GuruCul)
(https://www.youtube.com/channel/UCh58iDM5jtj1lTwCSLIj19A?sub_confirmation=1)

Privacy Policy (https://gurucul.com/privacy-policy)