Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Threat Actor Profile

June 13, 2023 TLP:CLEAR Report: 202306131500

Threat Actor Profile: FIN11

Executive Summary

FIN11 is a cybercriminal group that has been active since at least 2016, originating from the Commonwealth of Independent States (CIS). While the group has historically been associated with widespread phishing campaigns, the group has shifted towards other initial access vectors. FIN11 often runs high-volume operations mainly targeting companies in various industries in North America and Europe for data theft and ransomware deployment, primarily leveraging CL0P (aka CLOP). The group has targeted pharmaceutical companies and other health care targets during the COVID-19 pandemic and continues to target the health sector. The group is behind multiple high-profile, widespread intrusion campaigns leveraging zero-day vulnerabilities. It is likely that FIN11 has access to the networks of far more organizations than they are able to successfully monetize, and choose if exploitation is worth the effort based on the location of the victim, their geographical location, and their security posture. This Threat Actor Profile provides information associated with FIN11, including recent campaigns, associated malware, CVEs exploited, and TTPs.

Impact to HPH Sector

Given FIN11's history of conducting widespread campaigns exploiting zero-day vulnerabilities in commonly used software in the Healthcare and Public Health (HPH) sector to steal data and deploy ransomware, HC3 recommends that healthcare organizations consider FIN11 a top priority for their security teams. While HC3 cannot confirm exactly how many and which CL0P ransomware attacks may be attributed to FIN11, HC3 has observed around 30 incidents involving CL0P ransomware in the U.S. HPH sector since 2021. These affected organizations either provided direct patient care or were considered health plans and/or payers. CL0P ransom demands typically range from a few hundred thousand dollars up to USD $10 million. Recently, researchers observed wide exploitation of a zero-day vulnerability in the MOVEit Transfer secure managed file transfer software attributed to FIN11. The list of organizations that have disclosed data breaches following these attacks include a national public healthcare system.

Industry Names

FIN11 activity has overlaps with the following industry names for the threat actor:

- Odinaff (Symantec)
- Sectoj04 (NSHC Group)
- TA505 (Proofpoint)
- TEMP.Warlock
- Lace Tempest (Microsoft)
- DEV-0950 (Microsoft, defunct)
- Hive0065 (IBM X-Force)
- Group G0092 (Mitre)

Analyst Comment: Microsoft tracks two separate threat actors affiliated with TA505: Spandex Tempest (formerly CHIMBORAZO) and Lace Tempest (previously DEV-0950). Only Lace Tempest is affiliated with FIN11. Furthermore, while the names FIN11 and TA505 have often been used interchangeably, Google-owned Mandiant (formerly FireEye) considers FIN11 a subset of activity under the TA505 group. The threat clusters tracked by Mandiant as UNC2546, UNC2582, and UNC4857 have been merged into FIN11.

Recent High-Profile Campaigns

- MOVEit Transfer Zero-Day Exploitation (since May 2023)
- PaperCut MF and NG Exploitation (since at least April 13, 2023)

- Accellion File Transfer Appliance (FTA) Zero-Day Exploitation (December 2020)
- Windows ZeroLogon Vulnerability Exploitation (October 2020)

Malware Associated with FIN11

- LEMURLOOT
- CLOP ransomware
- Vidar (low confidence)
- AsyncRAT (low confidence)
- MINEDOOR/ FRIENDSPEAK (aka Get2)
- MIXLABEL (aka SDBbot)
- FlawedAmmyy
- FlawedGrace (AKA GraceWire, BARBWIRE)
- ServHelper
- P2P RAT
- Raspberry Robin (low confidence)
- Cobalt Strike
- Truebot (AKA TRUECORE)
- AdFind
- Amadey
- Azorult (low confidence)
- BloodHound
- Mimikatz
- PowerSploit
- DEWMODE

Analyst Comment: Much of the malware listed above has historically been associated with FIN11 and may not be used by FIN11 today. For example, FIN11 was well known for using FlawedAmmyy, but the group has not been observed leveraging this malware since 2019. FIN11 has also historically deployed point-of-sale (POS) malware targeting financial, retail, restaurant, and pharmaceutical sectors.

General TTPs Associated with FIN11

- Fake download pages
- Spearphishing emails with malicious attachments and links
- Use of CAPTCHA challenge prior to delivering malicious document
- Re-compromising organizations after losing access
- Deployment of web shells
- Use of bulletproof hosting infrastructure
- Exploitation of zero-day vulnerabilities
- Ransomware deployment and data theft for monetization and extortion

Analyst Comment: Some of these TTPs listed above may no longer be employed by FIN11. Additionally, some TTPs may be associated with FIN11 partners, and not FIN11 itself.

CVEs Potentially Exploited by FIN11

- CVE-2023-34362 (MOVEit Transfer)
- CVE-2021-27101 (Accellion FTA)
- CVE-2021-27102 (Accellion FTA)
- CVE-2021-27103 (Accellion FTA)
- CVE-2021-27104 (Accellion FTA)
- CVE-2023-27350 (PaperCut MF and NG)
- CVE-2023-27351 (PaperCut MF and NG)
- CVE-2023-0669 (GoAnywhere MFT)
- CVE-2021-35211 (SolarWinds Serv-U)
- CVE-2022-1388 (F5 BIG-IP)
- CVE-2021-44228 (Log4J) – almost certain

Mitigations

Mandiant has produced a detailed MOVEit Containment and Hardening guide to assist organizations with responding to this critical vulnerability in Progress Software's MOVEit Transfer application discovered by the vendor on May 31, 2023, which could lead to escalated privileges and potential unauthorized access.

Additionally, CISA released Cybersecurity Advisory (AA23-158A) titled "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability" which provides information on the Cl0p Ransomware Gang, including detection methods for MOVEit Transfer exploitation and IOCs.

Related HC3 Products

Types of Cyber Threat Actors That Threat Healthcare (June 8, 2023)
https://www.hhs.gov/sites/default/files/types-threat-actors-threaten-healthcare.pdf

Healthcare Sector Potentially at Risk from Critical Vulnerability in MOVEit Transfer Software (June 2, 2023)
https://www.hhs.gov/sites/default/files/moveit-transfer-software-sector-alert.pdf

New Data Breaches from Cl0p and Lockbit Ransomware Groups (April 28, 2023)
https://www.hhs.gov/sites/default/files/cl0p-lockbit-new-data-breaches-sector-alert.pdf

Clop Allegedly Targets Healthcare Industry in Data Breach (February 22, 2023)
https://www.hhs.gov/sites/default/files/clop-allegedly-targeting-healthcare-industry-sector-alert.pdf

Analyst Note: Clop Ransomware (January 4, 2023)
https://www.hhs.gov/sites/default/files/clop-ransomware-analyst-note-tlpclear.pdf

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (April 26, 2022)
https://www.hhs.gov/sites/default/files/russia-threats-to-critical-infrastructure-alert.pdf

SDBBot Malware threat to US Healthcare Organizations (November 17, 2020)
https://www.hhs.gov/sites/default/files/sdbbot-analyst-note.pdf

References

A Truly Graceful Wipe Out (June 12, 2023)
https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/

Clop ransomware likely testing MOVEit zero-day since 2021 (June 8, 2023)
https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-testing-moveit-zero-day-since-2021/

CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability (June 7, 2023)
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft (June 2, 2023)
https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft

Accellion FTA Zero-Day Attacks Show Ties to Clop Ransomware, FIN11 (February 22, 2021)
https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/

Russia-Based Hackers FIN11 Impersonate Zoom to Conduct Phishing Campaigns (September 22, 2022)
https://www.infosecurity-magazine.com/news/russia-fin11-impersonate-zoom/

FIN11: Widespread Email Campaigns as Precursor for Ransomware and Data Theft (October 14, 2020)
https://www.mandiant.com/resources/blog/fin11-email-campaigns-precursor-for-ransomware-data-theft

FIN11 hackers jump into the ransomware money-making scheme (October 14, 2020)
https://www.bleepingcomputer.com/news/security/fin11-hackers-jump-into-the-ransomware-money-making-scheme/

FIN11 Hackers Spotted Using New Techniques In Ransomware Attacks (October 14, 2020)
https://thehackernews.com/2020/10/fin11-hackers-spotted-using-new.html

FIN11 e-crime group shifted to clop ransomware and big game hunting (January 16, 2020)
https://www.scmagazine.com/home/security-news/fin11-e-crime-group-shifted-to-cl0p-ransomware-and-big-game-hunting/

Meet FIN11, a cybercrime outfit going after pharma companies while leaning on extortion (October 14, 2020)
https://www.cyberscoop.com/fin11-ransomware-pharma-fireeye-cybercrime/

Twitter, Microsoft Threat Intelligence, @MsftSecIntel
https://twitter.com/MsftSecIntel/status/1665537730946670595

Clop ransomware uses TrueBot malware for access to networks (December 11, 2022)
https://www.bleepingcomputer.com/news/security/clop-ransomware-uses-truebot-malware-for-access-to-networks/

Mitre ATT&CK, Software, FlawedAmmyy (last modified July 18, 2022)
https://attack.mitre.org/software/S0381/

Mitre ATT&CK, Group, TA505 (last modified March 22, 2023)
https://attack.mitre.org/groups/G0092/

A Look Inside TA505's ServHelper Malware Control Panel (September 6, 2022)
https://duo.com/decipher/a-look-inside-ta505-s-servhelper-malware-control-panel

TA505 Seen using P2P RAT in New Operations (December 1, 2021)
https://duo.com/decipher/ta505-seen-using-p2p-rat-in-new-operations

TA505's modified loader means new attack campaign could be coming (December 18, 2020)
https://intel471.com/blog/ta505-get2-loader-malware-december-2020/

FlawedAmmyy Malware Information (December 30, 2019)
https://success.trendmicro.com/dcx/s/solution/1123301-flawedammyy-malware-information

FIN11 aka TEMP.Warlock, UNC902
https://malpedia.caad.fkie.fraunhofer.de/actor/fin11

Microsoft Confirms PaperCut Servers Used to Deliver LockBit and Cl0p Ransomware (April 27, 2023)
https://thehackernews.com/2023/04/microsoft-confirms-papercut-servers.html

Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG (May 11, 2023)
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a

Odinaff: New Trojan used in high level financial attacks (October 11, 2016)
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=257dd693-5986-41bf-bc33-f9dc76d9c6a8&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Threat Actor Profile: TA505, From Dridex to GlobeImposter (September 27, 2017)
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter

Flowspec – TA505's bulletproof hoster of choice (July 15, 2020)
https://blog.intel471.com/2020/07/15/flowspec-ta505s-bulletproof-hoster-of-choice/

Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity (October 27, 2022)
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

Ransomware gang now using critical Windows flaw in attacks (October 9, 2020)
https://www.bleepingcomputer.com/news/security/ransomware-gang-now-using-critical-windows-flaw-in-attacks/

Five Eyes Agencies List Top 15 Most Exploited Bugs of 2021 (April 29, 2022)
https://www.infosecurity-magazine.com/news/five-eyes-list-top-bugs-2021/

Mandiant Red Team Emulates FIN11 Tactics To Control Operational Technology Servers (July 26, 2022)
https://www.mandiant.com/resources/blog/mandiant-red-team-emulates-fin11-tactics

HSE says 20 people's data breached in cyber-attack on third party recruitment software (June 9, 2023)
https://www.thejournal.ie/hse-cyber-attack-ey-thejournal-ie-6089340-Jun2023/

TA505 Continues to Infect Networks With SDBbot RAT (April 14, 2020)
https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback