F-SECURE THREAT HIGHLIGHTS REPORT

November 2021

F-Secure

EXECUTIVE SUMMARY

CONTENTS

MONTHLY HIGHLIGHTS

F-SECURE THREAT DATA HIGHLIGHTS

F-SECURE RESEARCH HIGHLIGHTS

FOREWORD

It is the end of November 2021, and the year is rapidly approaching its end. This month has been another busy one for interesting reporting and research being shared publicly across the industry. We start of this month's highlights focusing on the evolving trends of Iranian threat actors, before looking at the exploitation of another externally facing application by Chinese state-backed threat actors.

We continue our highlights by looking at the different evolutions amongst ransomware actors this month before rounding off with a brief overview of another fifteen notable reports we read this month. This section will continue in future versions of this report and hopefully serve as a good round up of the most useful reporting for the month in case you missed it.

The research highlight is a large one this month, with two F-Secure researchers releasing their findings of exploits of HP printers. There are two advisories and a technical paper to accompany these fully detailing this awesome research.

As always, we hope you enjoy this month's report, and we welcome any feedback you may have.

- Callum Roxan, Head of Threat Intelligence

MONTHLY HIGHLIGHTS

IRANIAN ACTORS: EVOLVING TRENDS

SUMMARY

Microsoft's MSTIC published two reports this month on Iranian threat actor activity. This first report was published on the MSTIC blog on the 16th November details newly observed TTPs being deployed by Iranian threat actors over the past year. The second report was published on the 18th November further identifies an increasing number of supply chain attacks conducted by Iranian threat actors against IT services organizations. The findings in both these reports indicate growing technical capability, operational persistence, and professionalization of Iranian threat actors over the past year.

In the first report on evolving trends in Iranian threat actors, MTSIC identify three trends in Iranian nation-state operators that have emerged during this period. Firstly, they are increasingly utilizing ransomware to either collect funds or disrupt their targets: they observed six Iranian TA's deploying ransomware in campaigns launched every six to eight weeks on average. PHOSPHORUS has been observed by MSTIC and DFIR Report exploiting vulnerabilities in Fortinet FortiOS SSL VPN (CVE-2018-13379) and on-premise Exchange Servers (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) as a vector to compromise. Once in the target environment the threat actor is reported to encrypts systems using BitLocker.

Secondly, they are more patient and persistent while engaging with their targets: both PHOSPHORUS and CURIUM were observed conducting social engineering activity to cultivate phishing targets with back-and-forth exchanges between the target and threat actor before delivering malware to the victim. The threat actor establishes trust and confidence with the target using alias profiles on social media or via email. By investing more time and effort engaging targets this increases the success rate of phishing campaigns and indicates an advancing social engineering techniques and persistence of these threat actors.

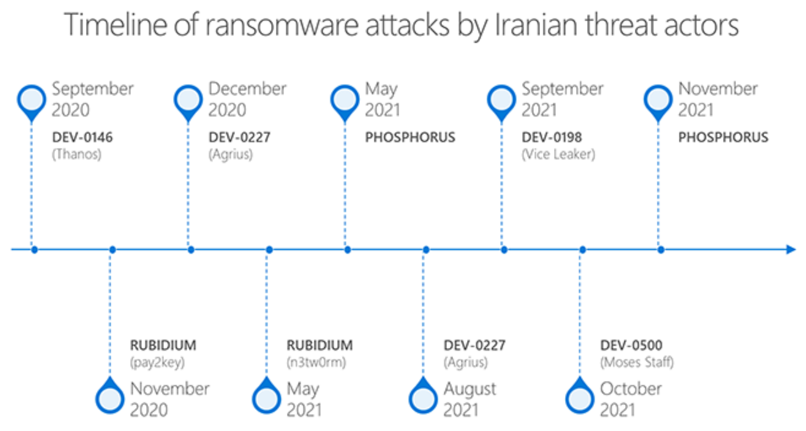


Figure 1: Timeline of ransomware attacks by Iranian threat actors

Source: https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

Thirdly, Iranian threat actors also continue to deploy aggressive brute force attacks against their targets. MSTIC observed DEV-0343 targeting Office 365 tenants in ongoing password spray attacks. Analysis of Office 365 logs suggests that DEV-0343 is using a red team tool like o365spray to conduct these attacks.

MSTIC assess these groups are operating in the interests of the Iranian regime. Its targets include defense companies that support United States, European Union, and Israeli government partners producing defense technology and geographic information systems (GIS) and transportation companies with a business focus in the Middle East.

The second report published on the 18th November found an increase in Iranian threat group activity targeting the IT sector in the past six months. Most of this targeting was focused on IT services companies based in India, as well as several companies based in Israel and United Arab Emirates. MSTIC assess these companies were secondary targets in supply chain attacks designed to steal credentials to enable onward further access to downstream customers in key sectors such as the defense and legal sectors of states of interest to the Iranian regime. Other targets include a government owned information and communication technology organization in the Middle East that supplies defense and transport sectors of interest to the Iranian regime.

MSTIC emphasized the significant uptick in activity from these groups they observed targeting Indian based service providers. They issued 1,788 notifications to Indian organizations between mid-August and late September, compared to just 10 notifications issued over the previous 10 years. MSTIC do note that they believe this activity is ultimately targeted at subsidiaries and clients outside of India.

For technical details and IOC's and detections relating to these campaigns refer to MSTIC's blog.

F-SECURE'S INSIGHT

Reporting on Iranian operations continues to suggest the evolution and increase in capability of these actors. The range of operations conducted in cyber space also appears to be expanding with information operations, disruption operations, and operations to provide capability support to physical operations also being reported.

To this aim, Iranian actors have been observed deploying a wider range of techniques including use of ransomware, disk wipers, mobile malware, social engineering and phishing attacks, password spraying, scanning and mass exploitation attacks, supply chain attacks and cloaking C2 communications behind legitimate cloud services.

These attacks demonstrate how Iranian state actors are following a trend in which state backed threat actors are increasingly targeting supply chains as indirect vectors to achieve their objectives. The utilization of ransomware to fund state activities appears to be a logical development of Iranian activity like that conducted by DPRK actors, a similarly heavily sanctioned nation.

The activity targeting Indian service providers is a notable event that organizations with these organizations in their supply chain. The use of Indian suppliers has long been seen as a cost-effective business decision, but one that now appears to carry additional risks that organizations need to factor into their risk management processes and strategic decision making. F-Secure would recommend organizations who may be interesting downstream targets for Iranian operators to look to put in place mitigations to manage this supply chain risk for their organizations.

DEV-0322: MANAGEENGINE EXPLOITATION

SUMMARY

This month, Microsoft reported exploits being used to compromise systems running the Zoho ManageEngine ADSelfService Plus Software. This software was vulnerable to CVE-2021-40539, a critical authentication bypass vulnerability in the REST API of the product that could lead to remote code execution.

Based on observed infrastructure, victimology, tactics, and procedures, Microsoft Threat Intelligence Center (MSTIC) attributes this campaign with high confidence to a group operating out of China, DEV-0322, which is the same threat actor MSTIC previously linked to attacks targeting the SolarWinds SERV-U software with another 0-day exploit. MSTIC assess this was a targeted campaign with victims in defense industrial base, higher education, consulting services, and information technology sectors.

Palo Alto unit 42 also reported on the similar activity they observed in a blog earlier this month. Unit 42 observed a threat actor uploading a payload after initial exploitation that installed the “Godzilla” webshell, which is an open-source Chinese language webshell. This activity was consistent across all victims, though a smaller number of victim organizations were then also targeted with a modified version of a new backdoor called NGLite, which is also developed with Chinese instructions and shared publicly.

Of note, Unit 42 identified the threat actor using a relatively novel technique for C2 communication. The backdoor NGLite, which is described by its authors as an “anonymous cross-platform remote control program based on blockchain technology”, uses New Kind of Network (NKN) for its C2 communication. Unit 42 researchers note they have seen only 13 samples communicating with NKN altogether – nine NGLite samples and four related to a legitimate open-source utility called “Surge” that uses NKN for file sharing.

The threat actor then moved laterally and ran commands within target environments using the Webshell or the NGLite payload. The actor exfiltrated files of interest, pivoted to a domain controller, and installed a new credential-stealing tool tracked as KdcSponge.

This is consistent with MSTIC observations that after initial exploitation of CVE-2021-40539 the threat actor performed credential dumping, installed custom binaries, and dropped malware to maintain persistence and move laterally. The threat actor also deployed a tool designed to read security event logs and look for EID 4624 logon events. The same tool would then collect domains, usernames, and IP addresses and write them to the file elrs.txt. After acquiring credentials, DEV-0322 was observed moving laterally to other systems on the network and dropping a custom IIS module.

In addition to a custom IIS module, the threat actor deployed a trojan MSTIC are calling “trojan:win64/zebracon”, which used hardcoded credentials to make connections to threat actor controlled Zimbra email servers.

Unit 42 assesses the TA’s objective is to establish persistence and data exfiltration of sensitive documents. They observed the threat actor transferring files to a staging directory and creating password-protected RAR archives in the recycler folder. These files were then downloaded from externally facing web servers.

Microsoft includes IOC’s and detections and hunting queries in their blog post

F-SECURE’S INSIGHT

MSTIC attributed this activity to the group they are tracking at DEV-0322 that they assess as highly likely a China based group. Earlier this year they also attributed compromise of SolarWinds Serv-U software with a 0-day exploits to this group. This would suggest a well-organized group with resources and capabilities to uncover vulnerabilities and develop exploits for operational use.

In an alert released by CISA no attribution was provided, but they did provide additional information on targets of this activity that spanned 16 critical infrastructure sectors. They identified some of those sectors as “academic institutions, defense contractors as well as transportation, information technology, manufacturing, communications, and finance”. The alert was released as a joint effort between the “Federal Bureau of Investigation (FBI), United States Coast Guard Cyber Command (CGCYBER), and the Cybersecurity and Infrastructure Security Agency (CISA)”. The inclusion of the CGCYBER can allow us to infer that some of the victims would have fallen under their remit and is probably linked to the inclusion of “transportation” victims in the report.

The alert also suggested the impact of the activity could “disrupt company operations/logistics and subvert U.S. research across critical infrastructure sectors”.

These statements from CISA gives credibility to the assessments provided by MSTIC. All the information available to F-Secure suggest that the activity described by MSTIC is that of a state-backed group. The activity and IOCs provided by MSTIC and Unit 42 have significant crossover; however, Unit 42 note that they believe the activity they observed was unrelated to the activity identified by the CISA alert. With the information provided it isn’t possible to make a high confidence assessment that this activity was from the same actor, *but F-Secure assesses that it is probably that the activity originated from the same geographic cluster of actors. This assessment can be supported by examining other clusters of exploitation activity earlier this year that showed the use of exploits by multiple actors from the same geographic region.*

RANSOMWARE: TRENDS AND NOTABLE REPORTS

SUMMARY

The focus of ransomware reporting this month are US government efforts to disrupt operations by placing sanctions against ransomware facilitators, offering six-figure rewards for ransomware affiliates and "key leaders". Reports by the FBI on how ransomware operators use reconnaissance activity to identify potential victims and analysis of TA505's exploitation of Serv-U vulnerabilities.

Ransomware Groups Leveraging 'Significant Financial Events' to Exploit Victims

The FBI published a TLP:WHITE report on ransomware groups use of "significant financial events" such as mergers and acquisitions to leverage victims for ransom payments. The report cites evidence such as second tier targeting of victims which they observe is based on the likelihood a victim will pay. The share price and financial events are a factor that are reportedly used by actors to qualify victims for further targeting and the FBI provided evidence of ransomware actors searching for or discussing financially related terms that may influence these decisions.

US Stepping Up Sanctions Against Ransomware Groups

The US Department of State announced a reward this month of up to 10 million USD for information leading to the identification of 'key leaders' of DarkSide ransomware or REvil organized crime groups and 5 million USD for information that leads to the arrest of affiliate members of these groups. At the same time, the US Department of Justice charged a Ukrainian and Russian citizens for their involvement in REvil attacks against Kaseya earlier this year. The US government has also taken further steps to disrupt ransomware operations by placing a second crypto exchange under sanctions for facilitating ransomware payments. The US treasury placed sanctions against Chatex for its direct ties with Suex, a Russian cryptocurrency exchange that was sanctioned in September for the same reason.

TA505 Exploiting SolarWinds Serv-U vulnerability

The NCC Group observed an increase in victims of the Clop ransomware over the past few weeks. NCC Group's research shows this uptick in activity is linked to a surge in activity exploiting a vulnerability in SolarWinds Serv-U file transfer Software. When exploited, the vulnerability CVE-2021-35211, allows the actor to spawn a sub-process that they control and allows them to execute further commands on the vulnerable hosts.

The report details how the actor used Base64 encoded PowerShell commands to deploy Cobalt Strike on the victim hosts and establish Command and Control (C2) communications. The actor hijacked a legitimate scheduled task to attempt to maintain persistence and deployed the FlawedGrace RAT.

See the full report for technical details on the attack as well as details around vulnerable versions and potential detection or investigation opportunities.

Other Ransomware Group Insights

Sophos released a report this month on an actor they track as "Memento team" who have been observed using Python-based ransomware that copies the victim's files to password protected archives before deleting the original files. This is a relatively simplistic technique compared to many modern ransomware families, and suggests an actor who is not operating with one of the main Ransomware as a Service (RaaS) operations.

Additionally, Prodaft released a detailed report into the prominent CONTI ransomware group. The report provides insights on how the group operates, its business model and its C2 infrastructure. The report is full of detail for defenders to pick over and digest to better develop mitigations to this prolific group.

F-SECURE'S INSIGHT

By placing rewards for information that leads to the arrest of members of DarkSide and REvil and their leadership, the US government is sending a clear signal of intent that they are taking real action against these groups. DarkSide had infrastructure taken down and suffered financial losses following FBI investigations into the Colonial Pipeline incident which was attributed to DarkSide. Following intense scrutiny from the FBI, DarkSide ceased operations.

In October's THR, we reported Emsisoft researchers found BlackMatter ransomware was almost identical to DarkSide suggesting they are likely the same threat actor or formed by some of the same individuals. This indicates the group has taken steps to rebrand following loss of infrastructure, finances, and credibility. Their operations have been disrupted again and BlackMatter is reported to have stopped operations. Further, as we have seen with recent arrests and takedowns of members of REvil, individual members are at risk of arrest and with rewards for their arrest this only increases the scrutiny and pressure on these individuals. Law enforcement and ransomware groups continue to play a game of cat-and-mouse but tangible results such as these will certainly serve as a deterrent to these groups.

OTHER NOTABLE HIGHLIGHTS IN BRIEF

SUMMARY

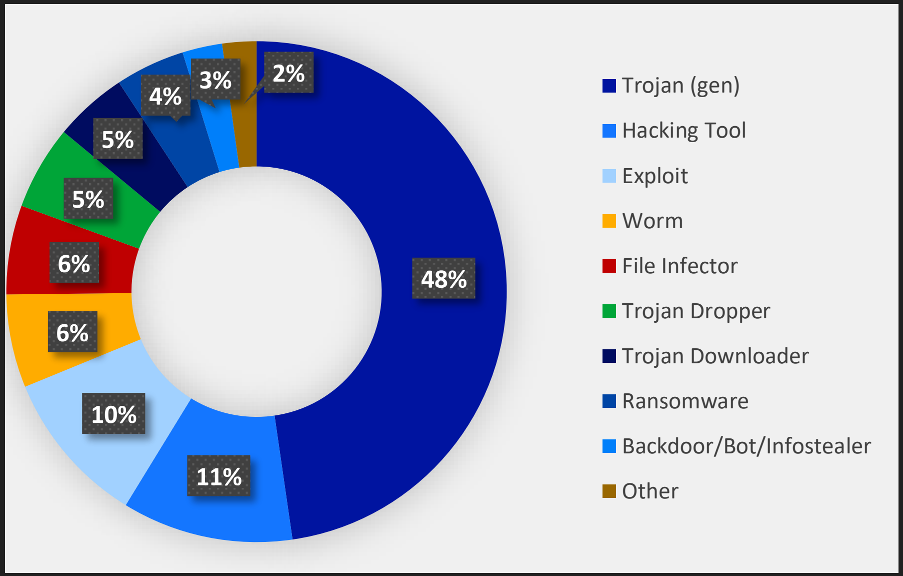
November was another busy month for interesting reporting and insights being published. While we cannot cover all these highlights in depth, we have included a brief listing of other interesting highlights from this month below:

- Google released a Threat Horizons report to help organizations protect their cloud environments from evolving threats
- Europol released their Internet Organised Crime Threat Assessment (IOCTA) 2021 report that focuses on evolving threats and key developments in the cybercrime space
- The European Union Agency for Cybersecurity (ENISA) released their 2021 threat landscape report
- Nokia have released their 2021 Threat Intelligence report, which understandably has good coverage of mobile related threats
- Intezer release a report identifying a new type of supply chain attack they describe as ChainJacking
- Proofpoint release an excellent report on a DPRK actor they track as TA406, who conducts information gathering attacks globally
- Kaspersky shared a report on the DPRK actor "ScarCruft" who has been targeting defectors and human rights activists
- The NSO group, amongst others, had export controls placed on them by the US government
- The Atlantic group released a report on the proliferation of surveillance technology at international arms markets and events
- ESET researchers uncovered the Lazarus group backdooring IDA Pro to compromise researchers and cybersecurity practitioners
- Trend Micro released a report detailing their analysis of a cyber-mercenary actor they track under the moniker "Void Balaur"
- Google released a report on an actor using watering hole attacks to exploit macOS users accessing Hong Kong media websites
- The FBI released a report on a threat actor exploiting a 0-day in FatPipe WARP, MPVPN and IPVPN Software
- An individual shared a report detailing technical analysis of APT31's SoWaT router implant
- Kaspersky published a report of activity of the "WIRTE" threat actor in their operations in the middle east

F-SECURE THREAT DATA HIGHLIGHTS

THREAT TYPES

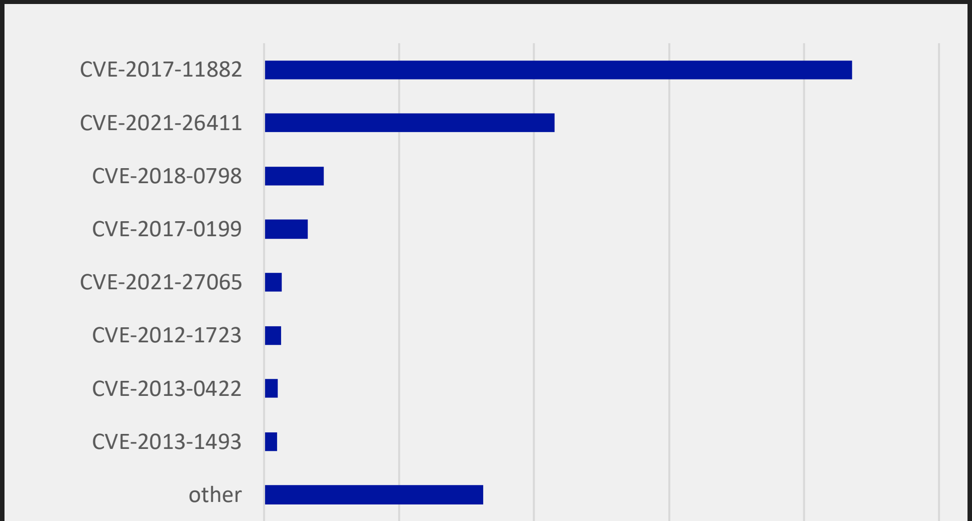
In November, various hacking tools and exploits have been the most prevalent identified threat. Detected hacking tools include software such as Mimikatz. Equation group tools contribute to biggest share of detected hacking tools.



EXPLOITS

CVE-2017-11882 exploits vulnerability in MS office products and provides remote code execution for the attacker. Most common attack vector is via email campaigns. It remains the most popular vulnerability against endpoints. This attack can be mitigated by updating the MS office with latest security updates.

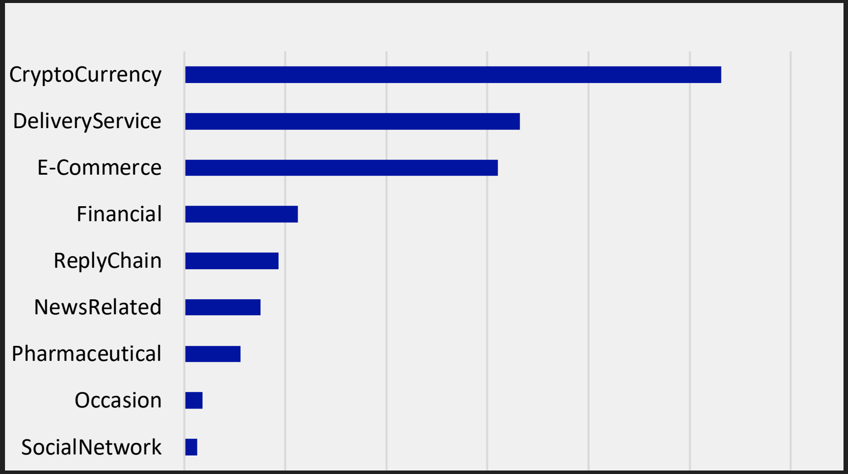
CVE-2021-26411 internet explorer memory corruption vulnerability follows at the second place.



SPAM EMAIL THEMES

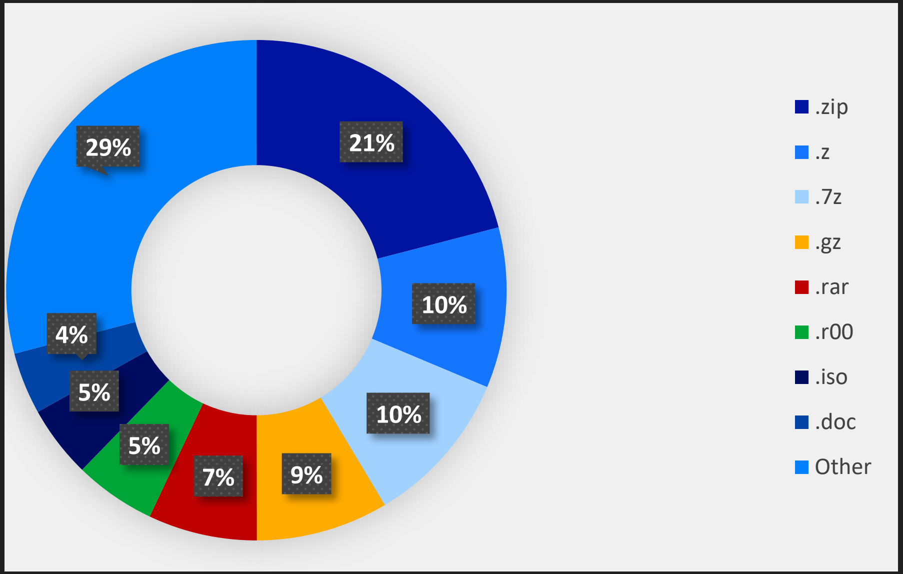
Cryptocurrency themes dominate the spam landscape followed by delivery service and E-Commerce.

FBI has released a public service announcement regarding increasing number of cryptocurrency scams leveraging crypto ATMs and QR codes for payment.
https://www.ic3.gov/Media/Y2021/PSA211104



MALICIOUS EMAIL ATTACHMENTS

In November, .zip attachments in emails were particularly prevalent followed by other archive formats.
Majority of the .zip volume is attributable to Agent Tesla campaigns where the malware is delivered within archives such as .zip & .gz.



F-SECURE RESEARCH HIGHLIGHTS

HP MULTI-FUNCTION PRINTER VULNERABILITIES

Two F-Secure researchers, Timo Hirvonen and Alexander Bolshev, recently discovered multiple vulnerabilities in HP Multi-Function printers. The two vulnerabilities are covered in full on the F-Secure LABS blog under two advisories CVE-2021-39237, CVE-2021-39238, and a longer research paper.

CVE-2021-39237

F-Secure found that HP multi-function printers (MFPs) have unlocked shells on the communications board connectors. A malicious actor with physical access to the device might be able to place a temporary or persistent implant via those interfaces. The interfaces in question are the Universal Asynchronous Receiver-Transmitter (UART) interfaces. One UART interface on the board provides access to the UEFI shell control, the other one to the root Linux shell of the scanner module. F-Secure found the issue on the HP MFP M725z model but there over 150 affected models.

The exploitability of the issue has not, however, been verified by F-Secure in any device other than the M725. The issue has been reported to the vendor and resolved in the latest versions of the firmware.

Malicious actors with physical access to the device can dump and tamper with all data that is stored on the system and user partitions of the device. It should be noted that the relevant connectors are large and easy to connect to, which greatly reduces the time and accuracy required for an attacker to connect the wires. The whole procedure of removing the connector board, connecting wires, booting the printer, installing a persistent / in-memory implant, and then removing the wires can take less than five minutes, increasing the risk of someone using this attack. Successful exploitation of the issue gives the attacker full control over the device.

The impact of this would be allow an attacker to gain control over the printer software, steal documents that are being scanned or printed, attack other printers using a remote code execution vulnerability in the font parser, or move laterally through the connected network infrastructure.

F-Secure strongly encourages installing the firmware update. The list of affected HP MFP models and the instructions for obtaining the updated firmware can be found in HP's security bulletin.

CVE-2021-39238

F-Secure discovered a Remote Code Execution (RCE) vulnerability within the firmware of the HP MFP M725z device. The font parser library is vulnerable to a memory corruption issue due to improper validation of an array index (CWE-129). The issue can be exploited remotely using a Cross-Site Printing (XSP) vector as part of a drive-by or social engineering attack via workstations that can communicate directly with the devices' JetDirect service. It is also possible to trigger and exploit the vulnerability locally using the 'print from USB' feature.

Approximately 150 different HP MFP models are affected. However, the exploitability of the issue has not been verified by F-Secure in any device other than the M725. This has been reported to the vendor and the issue has been resolved in the latest versions of the firmware.

Successful exploitation of the issue gives the attacker full control over the device. The impact includes but is not limited to:

- Access to documents that are being scanned and printed
- Network pivoting
- If USB is enabled, access to the USB flash storage which users print from or scan to (this includes reading, tampering with, and infecting the files on the USB)
- Access to credentials stored on the device for, e.g., LDAP integration or network access
- As the exploit can be turned into a network worm, it is possible for a compromised MFP to infect other vulnerable MFPs whose TCP port 9100 can be reached.

There are multiple ways to mitigate the vulnerability. First, printing from USB is disabled by default and should stay that way, as recommended by HP. Second, since an attacker in the same network segment can exploit the vulnerability by communicating directly to JetDirect TCP/IP port 9100, we recommend placing the printers into a separate, firewalled VLAN. All workstations should communicate with a dedicated print server, and only the print server should talk to the printers. This is important since, without proper network segmentation, the vulnerability could be exploited by a malicious website that sends the exploit directly to port 9100 from the browser.

To hinder lateral movement and Command & Control communications from a compromised MFP, outbound connections from the printer segment should be allowed only to explicitly listed addresses.

Finally, we recommend following HP's best practices for securing access to device settings to prevent unauthorized modifications to any security settings. They have an excellent technical white paper titled "HP Printing Security Best Practices for HP FutureSmart Products". This describes the process of using HP Web Jetadmin to secure all printers at the same time.

F-Secure strongly encourages installing the firmware update. The list of affected HP MFP models and the instructions for obtaining the updated firmware can be found in HP's security bulletin.

Disclosure Timeline

Date	Summary
2021-04-29	F-Secure notified HP of vulnerabilities
2021-05-12	Vendor acknowledged issue
2021-06-14	HP sends F-Secure a fixed firmware for verification
2021-11-01	HP publishes their Security Bulletins
2021-11-03	F-Secure confidentially informs clients to patch
2021-11-30	F-Secure publishes public advisory

F-Secure®

f-secure.com/ | twitter.com/fsecure | linkedin.com/f-secure-corporation