Jun 11 2023

NETMANAGEIT

Intelligence Report

Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG

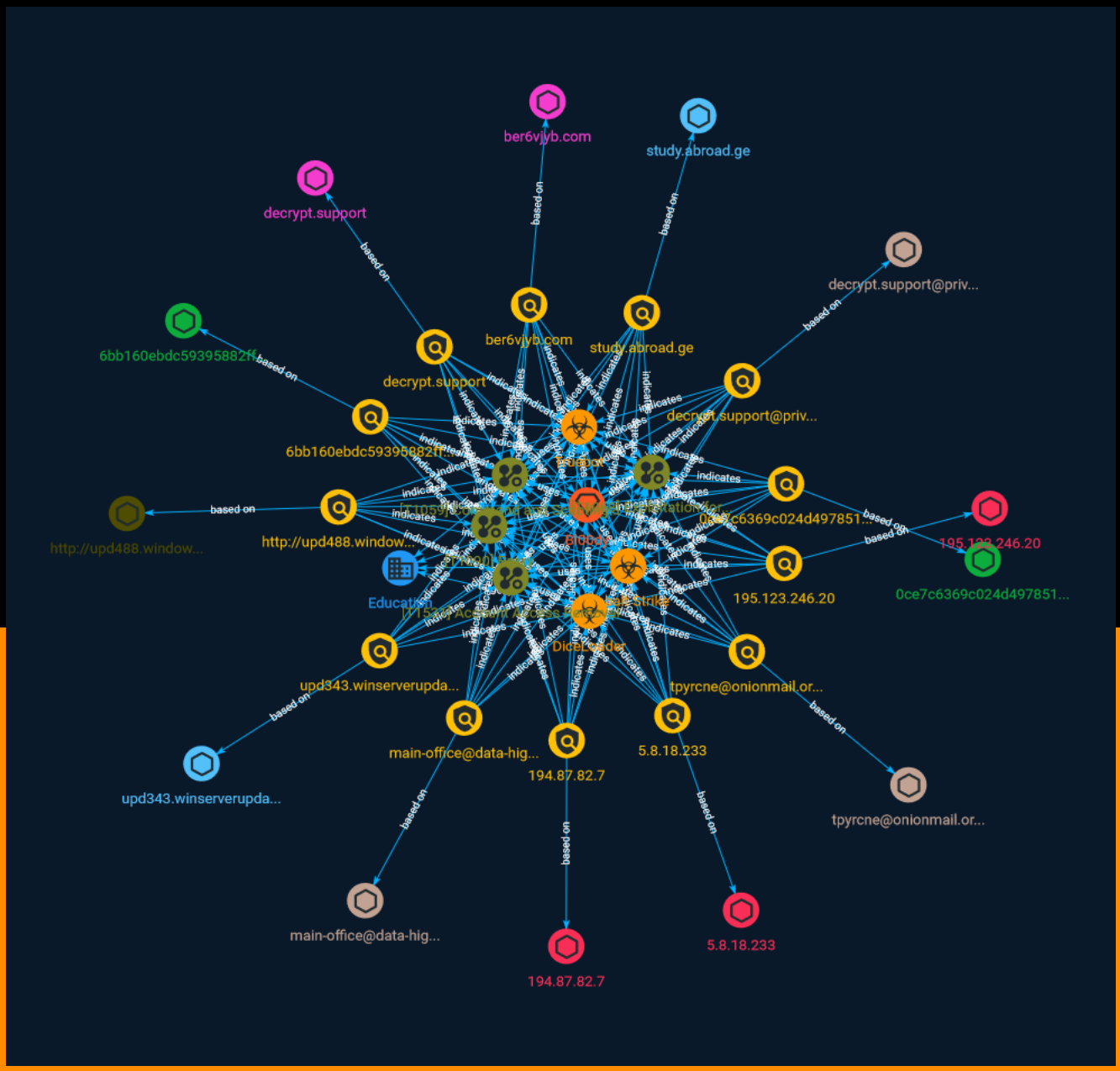

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The FBI and CISA have issued a joint cybersecurity advisory following the active exploitation of a vulnerability in PaperCut NG and Paper cut MF servers, which allows unauthenticated users to execute malicious code remotely.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name
Proxy
ID
T1090
Description
Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.
Name
Exploitation for Privilege Escalation
ID
T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Account Access Removal

ID

T1531

Description

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://

attack.mitre.org/techniques/T1529) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019) In Windows, [Net](https://attack.mitre.org/software/S0039) utility, `Set-LocalUser` and `Set-ADAccountPassword` [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets may be used by adversaries to modify user accounts. In Linux, the `passwd` utility may be used to change passwords. Accounts could also be disabled by Group Policy. Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Defacement](https://attack.mitre.org/techniques/T1491), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) objective.

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.

(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Sector

Name
Education
Description
Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.

Indicator

Name
study.abroad.ge
Pattern Type
stix
Pattern
[hostname:value = 'study.abroad.ge']
Name
5.8.18.233
Description
ISP: IP Volume inc **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` ``` ---------- **443:** ``` ``` ----------
Pattern Type
stix
Pattern

[ipv4-addr:value = '5.8.18.233']

Name

6bb160ebdc59395882ff322e67e000a22a5c54ac777b6b1f10f1fef381df9c15

Description

Win.Trojan.ChaChi-9910803-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6bb160ebdc59395882ff322e67e000a22a5c54ac777b6b1f10f1fef381df9c15']

Name

0ce7c6369c024d497851a482e011ef1528ad270e83995d52213276edbe71403f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0ce7c6369c024d497851a482e011ef1528ad270e83995d52213276edbe71403f']

Name

main-office@data-highstream.com

Pattern Type

stix

Pattern

[email-addr:value = 'main-office@data-highstream.com']

Name

ber6vjyb.com

Pattern Type

stix

Pattern

[domain-name:value = 'ber6vjyb.com']

Name

tpyrcne@onionmail.org

Pattern Type

stix

Pattern

[email-addr:value = 'tpyrcne@onionmail.org']

Name

http://upd488.windowservicecemter.com/download/update.dll

Pattern Type

stix

Pattern

[url:value = 'http://upd488.windowservicecemter.com/download/update.dll']

Name

decrypt.support@privyonline.com

Pattern Type

stix

Pattern

[email-addr:value = 'decrypt.support@privyonline.com']

Name

194.87.82.7

Description

ISP: Serverion LLC **OS:** None ---------- Hostnames: - ib.systems ---------- Domains: - ib.systems ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDvZAxybWSg6NSWFWM50TgnhFXRNy00p7eYmuo6BzNErgG4 skL63tBZyfLyRwBxvqOH/MUKcjig/50FUCIBnFKO3WWhEsY1LcjCo01Za3PANcjFtv3uRt563nFI YAVcZSRgcuLkBUtUjZxGgMEGPNs6PrDmeGk18Uzeq3gUeyHtI7WmbPl1X2jZ81vxMbzSTb3hkuxq IbsQUxIFnkajrO1lOPtOQc3861bsNH1pE+GWenm8JOOjluZTuNTm1gaK/fte7G4d05dRMiVac92J PFhEvKA0YaJqYDeCGHSswJvzg0Y0Yvs9+IVW+6QwljoIOl7WYXumg1fiC9aMXjRf2ocx1ypeG1kB 4fbCcBliiK1VsuanxWjaIZJyVkQgbZvxiFT6avsq1u+ZY9+sfHtcRliYKboPz5uMHSyWSRY7YSMI NZZQYWDcHFl7SbHReN+yZ7ZNQDiG7DBEiptiALnXp84TTl3NIk1faABsWhLY1rN01RiH/rKwm/3w GfjUfeVs10U= Fingerprint: a6:44:f9:ad:8d:65:5c:62:f7:90:ac:5b:7a:38:b1:70 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-

sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Sun, 23 Apr 2023 08:56:41 GMT Server: Apache/2.4.46 (Win64) Content-Length: 46 Connection: Close Content-Type: text/html; charset=iso-8859-1 ``` ---------- **443:** ``` \xff\xff\xff\xff ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.87.82.7']

Name

decrypt.support

Pattern Type

stix

Pattern

[domain-name:value = 'decrypt.support']

Name

195.123.246.20

Description

ISP: GREEN FLOID LLC **OS:** None ---------- Hostnames: - vds1104928.hosted-by-itldc.com ---------- Domains: - hosted-by-itldc.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDKaTbnaUusj4GUBrBItc6NDx/ehvumqlZuo4A5yJZYws/7 +XbAJF1ZzCrqny6pN2oWEXbf5y7qk+eTWeadadGu83P6N4P3yrbRW1r0cknCzwyp2M7Lg1xWCUOs Y48gQ4zSSHJIs2L4v+YCs6F+JeKYzmfyVrqlPr2vAW1DZjdZt4J1Cn9mPyaLSTxiHCo0RcuWlzxG KiIOGh9FHkLIWxdmLVzzBIN2CggcJ4SFW7HL8YcokH8J+uaXiBiocpD509BMNxS9ni1DDfG/iSkp 0PnBoMRX6/hxQdnRMubKMfoBmTC+tbjTgDSX0tG187+Sm046U5uE4Y/s3Uyhod+QL4ibGagZpllG Cw5DU6VgBbkWBtCoKFQeknH8uEYEegxp38Q730txFVB9grkdb9djFe4lfxgjWtg9NvfA2wW3QdbK ninwTSZrEKcOMzHd+FcAPZJtHdIKNlS7xfzsKVISIVyIfBdQ6nYLY0axQ/g/3CwjsLuEHsrd+cPJ qhINScp6TD0= Fingerprint: d9:13:73:fa:7f:9f:92:b0:b3:61:35:0b:fe:78:c0:d7 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Thu, 11 May 2023 08:49:56 GMT Server: Apache/2.4.46 (Win64) Content-Length: 46 Connection: Close Content-Type: text/html; charset=iso-8859-1 ``` ---------- **443:** ``` \xff\xff\xff\xff ``` ----------

Pattern Type
stix

Pattern
[ipv4-addr:value = '195.123.246.20']

Name
upd343.winserverupdates.com

Pattern Type

stix
Pattern
[hostname:value = 'upd343.winserverupdates.com']

Intrusion-Set

Name
Bl00dy

Malware

Name
DiceLoader
Name
Truebot
Name
Cobalt Strike
Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

Domain-Name

Value
decrypt.support
ber6vjyb.com

Email-Addr

Value
decrypt.support@privyonline.com
main-office@data-highstream.com
tpyrcne@onionmail.org

StixFile

Value
6bb160ebdc59395882ff322e67e000a22a5c54ac777b6b1f10f1fef381df9c15
0ce7c6369c024d497851a482e011ef1528ad270e83995d52213276edbe71403f

Hostname

Value
study.abroad.ge
upd343.winserverupdates.com

IPv4-Addr

Value
195.123.246.20
194.87.82.7
5.8.18.233

Url

Value
http://upd488.windowservicecemter.com/download/update.dll

External References

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a
- https://otx.alienvault.com/pulse/645e41ad40119c9b4d3e920e