



The Threat Actors Exploiting F5 Misconfiguration

Executive Summary

For years, F5 Networks, Inc., a multi-cloud application services and security company's BIG-IP software and hardware, have been subject to exploitation of its vulnerabilities by various threat actors. The company's product suite offers various services, including load balancing, DNS, and connectivity for network applications. Its ability to handle high-bandwidth interactions makes it popular among large enterprises and governments, both key targets of both nation-state and cybercrime groups. For this reason, any vulnerability is a significant security risk for F5's BIG-IP users, as well as third parties whose personal and financial information may be stored on or processed by a vulnerable device. What follows is an overview of the known vulnerabilities, the threat actors that exploit them, a summary of previous cybersecurity advisories concerning F5, MITRE ATT&CK tactics, techniques, and procedures, indicators of compromise, and defense and mitigation recommendations.

Overview of Vulnerabilities

NVD Published Date	Vulnerability	Description
October 26, 2023	CVE-2023-46748	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility that may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
October 26, 2023	CVE-2023-46747	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
May 5, 2022	CVE-2022-1388	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
July 1, 2020	CVE-2020-5902	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

Threat Actors

CVE-2023-46748

As of late October 2023, F5 reported that it observed unnamed "skilled" threat actors actively exploiting two recently disclosed and patched vulnerabilities, designated CVE-2023-46747 and CVE-2023-46748. F5 advised that these unnamed threat actors were able to delete signs of their malicious activity on compromised devices. This makes it virtually impossible to determine if a device has been compromised.

CVE-2023-46747

During the course of an intrusion investigation in late October 2023, Mandiant observed novel N-day exploitation of CVE-2023-46747 affecting F5 BIG-IP Traffic Management User Interface. Additionally, in February 2024, it observed exploitation of Connectwise ScreenConnect CVE-2024-1709 by the same actor. This mix of custom tooling and the SUPERSHELL framework leveraged in these incidents is assessed with moderate confidence to be unique to a People's Republic of China (PRC) threat actor, UNC5174.





Mandiant assesses UNC5174 (believed to use the persona "Uteus") is a former member of Chinese hacktivist collectives, which has since shown indications of acting as a contractor for China's Ministry of State Security (MSS) focused on executing access operations. UNC5174 has been observed attempting to sell access to U.S. defense contractor appliances, UK government entities, and institutions in Asia in late 2023 following CVE-2023-46747 exploitation. In February 2024, UNC5174 was observed exploiting a ConnectWise ScreenConnect vulnerability (CVE-2024-1709) to compromise hundreds of institutions primarily in the U.S. and Canada.

UNC5174 has been linked to widespread aggressive targeting and intrusions of Southeast Asian and U.S. research and education institutions, Hong Kong businesses, charities and non-governmental organizations (NGOs), and U.S. and UK government organizations during October and November 2023, as well as in February 2024.

	UNC5174 at a Glance	
Summary	UNC5174, a Chinese state-sponsored threat actor, has been identified for exploiting critical vulnerabilities in F5 BIG-IP and ScreenConnect. UNC5174 is believed to have connections to China's Ministry of State Security and has been observed using custom tooling and the SUPERSHELL framework in their operations. The actor has shown indications of transitioning from hacktivist collectives to working as a contractor for Chinese intelligence agencies.	
Aliases	Uteus	
Country of Origin	The People's Republic of China	
Motivation	Enabling espionage operations	
Target Countries	The United States, the United Kingdom, Germany, Sweden, Iran, Australia, Hong Kong, South Korea, and other Southeast Asia nations.	Source: Red Hot Cyber
Target Sectors	Education, private research and businesses, charities, and non- governmental organizations	

CVE-2022-1388

In August 2024, the Federal Bureau of Investigation (FBI), CISA, and the Department of Defense Cyber Crime Center (DC3) released a joint Cybersecurity Advisory (CSA) to warn network defenders that a group of Iran-based cyber actors continues to exploit U.S. and foreign organizations. This includes organizations across several sectors in the U.S. (including in the education, finance, healthcare, and defense sectors as well as local government entities) and other countries (including in Israel, Azerbaijan, and the United Arab Emirates).

The FBI assesses a significant percentage of these threat actors' operations against U.S. organizations are intended to obtain and develop network access to then collaborate with ransomware affiliate actors to deploy ransomware. The FBI further assesses these Iran-based cyber actors are associated with the Government of Iran (GOI) and—separate from the ransomware activity—conduct computer network exploitation activity in support of the GOI (such as intrusions enabling the theft of sensitive technical data against organizations in Israel and Azerbaijan).

The Iranian cyber actors' initial intrusions rely upon exploits of remote external services on internet-facing assets to gain initial access to victim networks. The Iran-based cyber actors have historically exploited





organizations by leveraging CVE-2022-1388 related to BIG-IP F5 devices.

CVE-2020-5902

The publication of this vulnerability initially stirred high interest among threat actors. Soon, cybercriminals on underground hacking forums started discussing techniques to enumerate and exploit vulnerable instances. In one instance, a user on a Russian-speaking forum discussed "Google Dorking" techniques to find vulnerable BIG-IP servers indexed by the search engine.

Subsequently, after the publication of the vulnerability's security advisory, the FBI followed up in early August by issuing a notification that it detected Iranian threat actors attempting to exploit the vulnerability since July. Further reports from security researchers confirmed that Iranian threat actor Pioneer Kitten had been observed exploiting the vulnerability to achieve initial compromise on their targets, and had begun selling access to compromised networks on dark web forums.

	PIONEER KITTEN at a Glance	
Summary	PIONEER KITTEN is an Iran-based adversary that has been active since at least 2017 and has a suspected nexus to the Iranian government. This adversary appears to be primarily focused on gaining and maintaining access to entities possessing sensitive information of likely intelligence interest to the Iranian government.	
Aliases	PARISITE, UNC757, Fox Kitten	
Country of Origin	The Islamic Republic of Iran	
Motivation	Enabling espionage operations	
Target Countries	Israel, Middle East North Africa (MENA), and North America, including the United States.	
Target Sectors	Technology, government, defense, and healthcare	Source: CrowdStrike

Previous Cybersecurity Advisories

In the past four years, both the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) have released cybersecurity advisories regarding the vulnerabilities of BIG-IP devices that have the potential to be exploited by threat actors.

Alert CISA Adds Two Known Exploited Vulnerabilities to Catalog
Date: October 31, 2023
Summary
CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.
CVE-2023-46747 F5 BIG-IP Authentication Bypass Vulnerability CVE-2023-46748 F5 BIG-IP SQL Injection Vulnerability
These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise. Note: To view other newly added vulnerabilities in the catalog, click on the arrow in the "Date Added to Catalog" column—which will sort by descending dates.
Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the Known Exploited Vulnerabilities Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet for

more information.





Alert CISA Adds Two Known Exploited Vulnerabilities to Catalog

Although BOD 22-01 only applies to FCEB agencies, CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice. CISA will continue to add vulnerabilities to the catalog that meet the specified criteria.

Cybersecurity Advisory Threat Actors Exploiting F5 BIG IP CVE 2022 1388
Date: October 12, 2022 Alert Code: AA22-138A Link
Summary
The Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing & Analysis Center (MS- ISAC) are releasing this joint Cybersecurity Advisory (CSA) in response to active exploitation of CVE-2022-1388. This recently disclosed vulnerability in certain versions of F5 Networks, Inc., (F5) BIG-IP enables an unauthenticated actor to gain control of affected systems via the management port or self-IP addresses. F5 released a patch for CVE-2022-1388 on May 4, 2022, and proof of concept (POC) exploits have since been publicly released, enabling less sophisticated actors to exploit the vulnerability. Due to previous exploitation of F5 BIG-IP vulnerabilities, CISA and MS-ISAC assess unpatched F5 BIG-IP devices are an attractive target; organizations that have not applied the patch are vulnerable to actors taking control of their systems.
According to public reporting, there is active exploitation of this vulnerability, and CISA and MS-ISAC expect to see widespread exploitation of unpatched F5 BIG-IP devices (mostly with publicly exposed management ports or self IPs) in both government and private sector networks. CISA and MS-ISAC strongly urge users and administrators to remain aware of the ramifications of exploitation and use the recommendations in this CSA—including upgrading their software to fixed versions—to help secure their organization's systems against malicious cyber operations. Additionally, CISA and MS-ISAC strongly encourage administrators to deploy the signatures included in this CSA to help determine whether their systems have been compromised. CISA and MS-ISAC especially encourage organizations who did not patch immediately or whose F5 BIG-IP device management interface has been exposed to the internet to assume compromise and hunt for malicious activity using the detection signatures in this CSA. If potential compromise is detected, organizations should apply the incident response recommendations included in this CSA.
Technical Details
CVE-2022-1388 is a critical iControl REST authentication bypass vulnerability affecting the following versions of F5 BIG-IP:
16.1.x versions prior to 16.1.2.2 15.1.x versions prior to 15.1.5.1 14.1.x versions prior to 14.1.4.6 13.1.x versions prior to 13.1.5 All 12.1.x and 11.6.x versions

An unauthenticated actor with network access to the BIG-IP system through the management port or self IP addresses could exploit the vulnerability to execute arbitrary system commands, create or delete files, or disable services. F5 released a patch for CVE-2022-1388 for all affected versions—except 12.1.x and 11.6.x versions—on May 4, 2022 (12.1.x and 11.6.x versions are end of life [EOL], and F5 has stated they will not release patches).

POC exploits for this vulnerability have been publicly released, and on May 11, 2022, CISA added this vulnerability its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. Due to the POCs and ease of exploitation, CISA and MS-ISAC expect to see widespread exploitation of unpatched F5 BIG-IP devices in government and private networks.

Cybersecurity Advisory	Threat Actor Exploitation of F5	BIG IP CVE 2020 5902
Date: July 24, 2020	Alert Code: AA20-206A	Link
	Summary	
The Cybersecurity and Infrastructure Security	Agency (CISA) is issuing this alert i	in response to recently disclosed exploits the
target F5 BIG-IP devices that are vulnerable to	o CVE-2020-5902. F5 Networks, Ir	nc. (F5) released a patch for CVE-2020-590
on June 30, 2020. Unpatched F5 BIG-IP device	ces are an attractive target for mal	licious actors. Affected organizations that hav
not applied the patch to fix this critical remote	e code execution (RCE) vulnerabilit	tyrisk an attacker exploiting CVE-2020-590
to take control of their system. Note: F5's sec	curity advisory for CVE-2020-5902	states that there is a high probability that an
remaining unpatched devices are likely alreated	ady compromised.	





Cybersecurity Advisory Threat Actor Exploitation of F5 BIG IP CVE 2020 5902

CISA expects to see continued attacks exploiting unpatched F5 BIG-IP devices and strongly urges users and administrators to upgrade their software to the fixed versions. CISA also advises that administrators deploy the signature included in this Alert to help them determine whether their systems have been compromised.

This Alert also provides additional detection measures and mitigations for victim organizations to help recover from attacks resulting from CVE-2020-5902. CISA encourages administrators to remain aware of the ramifications of exploitation and to use the recommendations in this alert to help secure their organization's systems against attack.

Technical Details

CISA has observed scanning and reconnaissance, as well as confirmed compromises, within a few days of F5's patch release for this vulnerability. As early as July 6, 2020, CISA has seen broad scanning activity for the presence of this vulnerability across federal departments and agencies—this activity is currently occurring as of the publication of this Alert.

CISA has been working with several entities across multiple sectors to investigate potential compromises relating to this vulnerability. CISA has confirmed two compromises and is continuing to investigate. CISA will update this Alert with any additional actionable information.

MITRE ATT&CK Techniques

PIONEER KITTEN

The following are tactics, techniques, and procedures (TTPs) that have been observed being used by PIONEER KITTEN in past incident repsonse engagements. The table below illustrates these TTPs according to the MITRE ATT&CK framework.

		Source: Picus Security		
Reconnaissance T1596		Search Open Technical Databases		
Initial Access	T1190	Exploit Public-Facing Application		
	T1505.003	Web Shell		
	T1136.001	Create Account (Local Account)		
Persistence	T1098	Account Manipulation		
	T1053	Scheduled Task/Job		
	T1505	Server Software Component		
Privilage Eccelation	T1078.003	Valid Accounts: Local Accounts		
Finilege Escalation	T1078.002	Valid Accounts: Domain Accounts		
Defense Evasion	T1562.001	Impair Defenses: Disable or Modify Tools		
Credential Access	T1056	Input Capture		
Execution	T1059.001	Command and Scripting Interpreter		
Discovery	T1012	Query Registry		
Discovery	T1482	Domain Trust Discovery		
Command and Control	T1219	Remote Access Software		
Command and Control	T1572	Protocol Tunneling		
Exfiltration and Impact	T1657	Exfiltration Over Web Service		

UNC5174

The following are tactics, techniques, and procedures (TTPs) that have been observed being used by UNC5174 in past incident repsonse engagements. The table below illustrates these TTPs according to the MITRE ATT&CK framework.



Health Sector Cybersecurity

Coordination Center

		Source: Mandiant		
Initial Access	T1190	Exploit Public-Facing Application		
	T1027	Obfuscated Files or Information		
	T1070.004	File Deletion		
Defense Evasion	T1140	Deobfuscate/Decode Files or Information		
	T1222.002	Linux and Mac File and Directory Permissions Modification		
	T1601.001	Patch System Image		
	T1016	System Network Configuration Discovery		
Discovery	T1049	System Network Connections Discovery		
Discovery	T1082	System Information Discovery		
	T1083	File and Directory Discovery		
	T1095	Non-Application Layer Protocol		
Command and Control	T1105	Ingress Tool Transfer		
	T1572	Protocol Tunneling		
	T1573.002	Asymmetric Cryptography		
Execution	T1059	Command and Scripting Interpreter		
Execution	T1059.004	Unix Shell		
Persistence	T1136.001	Local Account		
Impact	T1531	Account Access Removal		
Credential Access	T1003.008	/etc/passwd and /etc/shadow		
Resource Development	T1608.003	Install Digital Certificate		

Indicators of Compromise (IOCs)

The following are IOCs that have been observed being used per CVE in past incidents:

CVE-2023-46748

Mandiant IOCs				
	Network	IOCs		
IP Address	ASN	NetBlo	ck	Location
118.140.151[.]242	9304	HGC Global Communications Limited		(HK)
61.239.68[.]73	9269 Hong Kong Broadband Network Ltd.		(HK)	
172.245.68[.]110	36352	Colocre	ossing	(U.S.)
	URL	S		
URL Description				
http://172.245.68[.]110:8888	SUPERSHELL C2			
Host IOCs				
MD5 Hash	Filename		Туре	Code Family
c867881c56698f938b4e8edafe76a09b	LG		ELF	SNOWLIGHT
df4603548b10211f0aa77d0e9a172438	N/A		ELF	SNOWLIGHT
0951109dd1be0d84a33d52c135ba9c97	N/A		ELF	SNOWLIGHT
9c3bf506dd19c08c0ed3af9c1708a770	memfd:a		ELF	N/A
0ba435460fb7622344eec28063274b8a	Undefined		ELF	SNOWLIGHT
a78bf3d16349eba86719539ee8ef562d	N/A		ELF	SNOWLIGHT

CVE-2023-46747

Mandiant IOCs				
	Network	IOCs		
IP Address ASN NetBlock Location				

U.S. Department of Health and Human Services

Health Sector Cybersecurity Coordination Center (HC3) www.HHS.GOV/HC3





Mandiant IOCs				
118.140.151[.]242 9304		HGC Global Communications Limited		(HK)
61.239.68[.]73	9269	Hong Kong Broadband Network Ltd.		(HK)
172.245.68[.]110	36352	Colocr	ossing	(U.S.)
	URL	S		
URL			Description	
http://172.245.68[.]110:8888	SUPERSHELL C2			
Host IOCs				
MD5 Hash	Filename		Туре	Code Family
c867881c56698f938b4e8edafe76a09b LG			ELF	SNOWLIGHT
df4603548b10211f0aa77d0e9a172438	N/A		ELF	SNOWLIGHT
0951109dd1be0d84a33d52c135ba9c97	N/A		ELF	SNOWLIGHT
9c3bf506dd19c08c0ed3af9c1708a770	memfd:a		ELF	N/A
0ba435460fb7622344eec28063274b8a	Undefined		ELF	SNOWLIGHT
a78bf3d16349eba86719539ee8ef562d	N/A		ELF	SNOWLIGHT

Phoenix Security IOCs

To check for IoCs associated with the SQL injection flaw in CVE-2023-46747 users are recommended to check the /var/log/tomcat/catalina.out file for suspicious entries like:

java.sql.SQLException: Column not found: 0.

sh: no job control in this shell

sh-4.2\$ <EXECUTED SHELL COMMAND>

sh-4.2\$ exit.

CVE-2022-1388

Unit42 IOCs
Payload SHA256
30f7e1998d162dfad69d6d8abb763ae4033bbd4a015d170b1ad3e20d39cd4e20
da647646cd36a3acb716b4266e9032f9c1caf555b7667e1dbe5bef89e7d2fdbb
b39d2a1202351d3be5d9906ec47ee05c305302124dddec5538dc7b9924c6b85d
ad6d44c70f83431bedf890967f2da0607c9b1f79591fb1b2697160f5b1c1a75c
1f93a6696f7bf1b2067cc503583deb4840404ebeeba89579bd303f57000baeb7
9a72aab2a3d1d6e66c185966597a52a8726ca25f5d9e2195af44f98d8b1847d5
53214f4d2d2dfd02b46f416cbdcb6f3a764820a50da4d59926f829b96cf82a6c
Source IPv4
20.187.67[.]224
192.132.218[.]149
85.203.23[.]73
116.48.110[.]159
Hosting URLs
hxxps://transfer[.]sh/dlxo3l/1.sh
hxxp://20.239.193[.]47/kele.sh
hxxp://20.239.193[.]47/kele1
hxxp://20.187.86[.]47/dadda
Cisco Talos Blog IOCs
IPs





Unit42 IOCs					
5[.]189[.]191[.]107	103[.]144[.]149[.]49	157[.]245[.]200[.]184	189[.]37[.]76[.]246		
29[.]104[.]233[.]152	103[.]177[.]174[.]34	157[.]245[.]206[.]99	189[.]46[.]90[.]233		
41[.]79[.]198[.]18	104[.]208[.]85[.]237	159[.]89[.]182[.]71	193[.]29[.]15[.]143		
45[.]61[.]139[.]143	104[.]244[.]72[.]174	161[.]35[.]156[.]235	194[.]163[.]164[.]206		
45[.]79[.]171[.]157	107[.]189[.]29[.]64	161[.]35[.]158[.]59	194[.]163[.]185[.]138		
51[.]159[.]66[.]249	109[.]205[.]176[.]248	161[.]35[.]209[.]168	194[.]195[.]219[.]144		
52[.]74[.]130[.]60	113[.]23[.]27[.]104	161[.]35[.]232[.]12	194[.]195[.]86[.]50		
53[.]85[.]187[.]67	113[.]67[.]10[.]13	163[.]143[.]106[.]199	194[.]233[.]171[.]91		
58[.]213[.]200[.]67	119[.]140[.]78[.]118	163[.]32[.]193[.]116	194[.]233[.]77[.]245		
64[.]39[.]106[.]34	12[.]172[.]214[.]26	164[.]90[.]205[.]93	194[.]5[.]73[.]6		
64[.]39[.]108[.]98	120[.]170[.]212[.]254	167[.]172[.]83[.]249	196[.]65[.]108[.]171		
64[.]39[.]98[.]152	120[.]245[.]25[.]3	167[.]172[.]83[.]250	198[.]211[.]120[.]110		
64[.]39[.]98[.]159	121[.]196[.]223[.]32	167[.]172[.]83[.]251	198[.]252[.]101[.]110		
64[.]39[.]98[.]196	122[.]161[.]50[.]64	167[.]99[.]225[.]132	204[.]195[.]115[.]184		
64[.]39[.]98[.]227	122[.]75[.]182[.]121	172[.]104[.]15[.]189	206[.]189[.]200[.]122		
64[.]39[.]98[.]40	124[.]160[.]154[.]32	172[.]70[.]126[.]146	207[.]180[.]241[.]85		
66[.]254[.]159[.]252	128[.]199[.]16[.]44	172[.]70[.]131[.]167	208[.]71[.]210[.]1		
66[.]94[.]126[.]14	132[.]145[.]21[.]77	172[.]70[.]131[.]47	209[.]58[.]170[.]164		
68[.]183[.]202[.]236	137[.]184[.]236[.]99	172[.]70[.]222[.]71	210[.]92[.]18[.]153		
69[.]24[.]129[.]229	139[.]99[.]149[.]66	172[.]81[.]129[.]138	212[.]102[.]50[.]210		
72[.]166[.]5[.]40	141[.]11[.]28[.]89	174[.]138[.]22[.]187	217[.]252[.]7[.]13		
72[.]167[.]51[.]207	141[.]11[.]28[.]97	175[.]107[.]236[.]67	223[.]187[.]119[.]114		
79[.]18[.]33[.]4	144[.]202[.]124[.]151	178[.]62[.]228[.]64	223[.]72[.]39[.]119		
81[.]69[.]58[.]15	144[.]202[.]59[.]76	180[.]236[.]169[.]125	226[.]137[.]152[.]105		
82[.]80[.]33[.]200	144[.]76[.]251[.]214	181[.]214[.]206[.]31	250[.]100[.]25[.]148		
87[.]20[.]54[.]33	145[.]215[.]56[.]53	185[.]147[.]212[.]58	253[.]240[.]199[.]27		
88[.]226[.]109[.]164	149[.]28[.]147[.]208	185[.]212[.]61[.]84	103[.]85[.]25[.]79		
91[.]36[.]121[.]76	150[.]230[.]38[.]225	185[.]239[.]226[.]177	156[.]34[.]23[.]233		
94[.]177[.]118[.]79	156[.]146[.]34[.]98	186[.]80[.]52[.]118			
103[.]144[.]149[.]206	157[.]245[.]115[.]135	188[.]68[.]61[.]6			

CVE-2020-5902

Trend Micro IOCs					
URLs					
URL		Description			
78.142.18.20		C&C server			
79.124.8.24		Disease vector			
S	HA256				
SHA256	Desc	ription	Detection Name		
acb930a41abdc4b055e2e3806aad85068be8d85e0 e0610be35e784bfd7cf5b0e	fetch.sh		Trojan.SH.MIRAI.BOI		
007254539d542563b4c4b66cee57cd1a49b5d4701 d43f83db908f198aaf48229					
af5cceefa2292b47042df22983d65c34fb57ff0f52fe 4135738c53079b699fd1	sora.arm7		Backdoor.Linux.BASHLITE.SMJC		
b2fe976028bf9b9b6f78c9461fd9e6389f41e357691 226be7c64a8f6e01b3cf9					
191cda060fa0e34cc46c616d1308df8914d8fe53c5c e3dc232bec56467adccc9					
03254e6240c35f7d787ca5175ffc36818185e62bdfc			Backdoor.Linux.MIRAI.VWIUP		

[TLP:CLEAR, ID:202410081500, Page 8 of 14]

U.S. Department of Health and Human Services

Health Sector Cybersecurity Coordination Center (HC3) www.HHS.GOV/HC3





Office of

Information Security

Securing One HHS

448836b3424451a747156d	Trend Micro	IOCs
b02b5f8a1eOcd51f9ef2383abc9362b83eba77bbd	4d88d5b342451a747156d	
b46:21913553637809f2e b b22d77244525448544306be4607242e45065632 c b70e3766271993388h3re4035566c5011afb4b1a c sale3e0803(re0c2592738 c b70e3766271993388h3re4035566c5011afb4b1a c sale3e0803(re0c2592738 c b70e3766271993388h3re4035566c5011afb4b1a c sale3e0803(re0c2592738 c b70e3766271933894h3de40526282ab74bbee c s863841h48455eed641 c c183c02de37bc29ea63cbe836447b3b12c0078e13 c c183c1b2de37bc29ea63cbe836447b3b12c0078e13 c c183c1b2de37bc29ea63cbe836447b3b12c0078e13 c c183c1b2de37bc29bc8310d27ca7 c c23arOrde6677ef7398d76a30330adf2321e547007 c b3b639211330c99636b84 c d6389431dac2cdar900323d5erbd4c1b9f3a68113 e 915985abe1fa7d64d7fd c d165828/cd80a25d7921e c 562864rd600253005H10cc1316c384037rc72419 c c6626001580c6410cc138534037rc72419 c c662820c533ubce911cec2146761b4c51d566a1 c s21183069d0514d820rc c 68	b02b5f8a1e0cd51f9fef2383ab2c9362b83ebab7bbd	
b22d7772c4d82554875d4306be4607242e45065632 b70e3766271993388b33te403556ec5011afb4b1a b3c1e3c80251e0c2592738 b9c281aac5d8abco2592738 b9c281aac5d8abco2592738 b3c3b2026d5c4c02371b73e4fb2dc282aab74bbee 3835b2d7a5bc29ea53cb836441p3b12c0078e13 0.41d03398c810d2d7a87 232bd7a7bead557c91116078a5b233b47878bab af0a1c7573e976c881s521 23a70ua657r7308d763303340adf2321e547007 b98e424933aec3ab456ea61 c57600234c55dc91139567920a0413011218e b3693521133005a96968b8 c45894611ac22c4a790303d40adf3221e547007 b98e424933aec3ab456ea61 c567600234c65dc91139567920a0431031b1218e b3693521133005a96968b8 c45894611ac22c4a790023d5e7b4ab6625 20b62c60dc0e7b45e972 56286d636065ce37671ac29f6987r44566d9b9b86778 08ba61200663325d7921e 555286dre3600523006f10cec318c3840377c72419 662a2c60116ce389e8b9 6222c32e5513b4ac911cec2148c76h4dc51d5e6a1 2321183309a0531d8207c 68884303be81b1627c6ac609866028c 72258b610702454b03be9772a17e9edc3c2251d2 562584107103c56c20580d13635f6705054773 92629e516702456b137682203b68759e73a ed300766b7048222e405	b46c9191355363f809f2e	
ferdder/a37(2725eb8e/770	b22d772c4d825548f5d4f306be460f242e45065632	
b70e3766271993388db37ee403556ec5011afb4b1a 5b42e30805re0c2592738 b92281ae56d8ebcc39939da7c5c4fd2538af924f11 0142de026b458e2dc7c 0f6aa4092e9dc5de0371673e4fb2dc282aab74bbee 38853841fb48d55eed644 1835db2dfe3fbe29ea63cbe33644f23b12c00f8f3 041403398c810u2d7a87 23b70rabe6777308d76c81c521 23b70rabe6777308d76c81c521 23r0rabe67777308d76c81c521 23r0rabe67777308d76c81c521 23r0rabe67777308d76c81c521 23r0rabe67777308d76c81c521 23r0rabe67777308d76c81c521 23r0rabe67777308d76c81c521 23r0rabe67777308d76c81c521 23r0rabe67787308d7630032d5e7bd4c1b9f368113 915985babe17af0c477d6 46589461d1a2c2cda790032d5e7bd4c1b9f368113 915985babe17af0c27f728d766db9b86778 08ba61200683f325d7921e 556286ford3600253f008c116cc31be23f6840377c72419 e6ac2690116ec589e3be9 6226532c653bdace911cec214676fb4551d566a1 33c1183d980a58118207 9b725296167d24584b03bba97c4e2829ba599465 42284301913a7cd5f99 a12xee1077008d07desc039f6203b68759e73a c6567b0f7a542546b1d6ef5a3385f670505477a4feb 0x	fefdde7a37f2725eb8e770	
5a1e302803(e0c2592738 Image: Control of Control	b70e3766271993388db3fee403556ec5011afb4b1a	
bpe2281aec5d8acbcc39939da7c5c4fd2538af924f11	5a1e3e0803fce0c2592738	
0142de026b4b58e2dfc7c df6aad092e9dc5dc0371673e4bb2dc282ab74bbe 388638f41fb48d55eed64f 183560b2dfe31bc22bea63cbe83644f2b3b12c00f8ef3 04t403398c63cb102df7a87 232bd7a7beads597ce711f607a8d58238b4f878bab af0a1cf375a976c681c521 23370da6677e77308d763d03340adf2321e547007 b98e424493aec3cb456ea61 267600324455dc31f395e87920a0431c31b1218ee b3b639521b350c9a6968b8 465894611da2ccdar790302d5e7b4dc1b9f3a68113 915P85abe1fa7dc64f7d6 4f05e822ce94a246e01acc0d001f9595d2b7ab8625 2b05c2d6dd0e7b45e9876 55c286fde73600253006f10eca18c3840377c72419 e6ac2690116ee589e8b9 622c632ec5b3bdae911eec2c14676bf4c51d5e6a1 33r18a34980a58148207c 688845103be8fbdab5cf3fbe9atc6ac6d9866028cc 37258b60fbc5c79c3c581 9b2622e6167024654003ba97c4e2c329ba599465 42ba43019b13e7cd51979 af2eae107008b004ce0097f2a17e9edc3c2251d2 5ef68ab7f103v96e2058048014369bc3321831 ec567b017a342c9b517d1cc c97008c7a8c44852c40552404388279823058759e73a ed5d047c103v95e22a005k6759e73a ed5d047c103v95e22a005k6759e73a ed5d047c82d53b52f7d7dc82c5858048074190566 163	b9e281aec5d8acbcc39939da7c5c4fd2538af924f11	
Iffead092e9dc5dc0371673e4fb2dc282ab74bbee 388638/41fb48d55eed64f I835db2fte3fbe29e63Cbe83644f2b3b12c00f8ef3 041403398c8a1042d7a87 232bd737bead597ce71303d763d03340adr2321e547007 b98e424933aec3cb456ea61 23704c677677303d763d03340adr2321e547007 b98e424933aec3cb456ea61 267600324455dcc91395687920a0431c31b1218ee b3639521b350c9a6968b8 46589461d1a2c2cb790032d5e7b4dc1b9f3a68113 915f885abe1fa7d6c4f7d6 47d5822c94a246e01afcc0001f9595d2b7ab8625 2b05c26d6d0e7bf45e9876 55c286dfc4f800025300061J0cca18c3840377c72419 e6ac2690116ee589e8be9 6226c32ac5b3bbace911cec214676fb14c51d5e6a1 83c1183d980a581d8207c 6888a5d3be8bbabbab6f3be9baf66028cc 7258b60hc5c79c3c581 902629e5167d24654003ba97c4e2c829ba599465 428e43801495132rcd591637068203b68759e73a ed6d904455e94a45821493 eff708c7a8dc465e1d6563a38ff670505477a4feb 0a376230e3100da5e687a eff80978bc373c588069002530068759e73a ed6d904455e94a45821492004dcfe4582588c1952d74dc82cf581c6c70 060b29eea4d15170b4398 1831113e67232b617d4c82cf581c662798 060b29eea4d15170b4398 183111	0142de026b4b58e2dfc7c	
388638/41/h48d55eed64/t (835db2/df3be29ea63cbe83644f2b3b12c00f8ef3 (04403398c6a10d2/ra67 232bU7a7beadb597ce711f607a8d58238b4f878bab (04167373976c681c521 23a70de6677e77308d763d03340adr2321e547007 b98e424493aec304b56ea61 267600324455dcs91f395e870200431c31b1218ee b3b639521b350c9a6968b8 46589461d1a2c2cdr390032d5e7bd4c1b9f3a68113 915985abe1fa7dc64f7d6 4fd582a2c942a246e1bacc0d105955d2b7ab8625 2b06c2e6de0e7bf45e9876 55a4d5a60c6ea47671e29f698ff7a4566d9b9b86778 08ba61200683f325d7921e 55a4d5a60bcea47671e29f698ff7a4566d9b9b86778 08ba61200683f325d7921e 55a4d5a60bcea47671e29f698ff7a4566d9b9b86778 08ba61200063f3125d7921e 55a4d5a60bce37671e29f698ff7a4566d99b9b86778 08ba61200063f312807c 6888a5d35be8fbbdab5ef3fbe9daf5ec36986028cc 37258b60hbc5r9c3c58f 902629e5167d24654003bba97c4e2c829ba599465 42b84301f913aercd5199 2f2cae1070038004ce05097c2a17e9edc3c2251d2 5ef5baba7c1975e07cee 297d08c7ac4465c126d5f5da385ff670505477a4feb 0a37c230e3100d3e687a 6d504345224055c3798203b68759e73a ed504455e94a45822493044cr6	df6aa4092e9dc5de0371673e4fb2dc282aab74bbee	
F835db2dfc3fb29pea63cbe83644f2b3b12c00f8cf3	388638f41fb48d55eed64f	
041403398c8a10/d2d7aE7	f835db2dfe3fbe29ea63cbe83644f2b3b12c00f8ef3	
232Dd7a7beads97ce7111607a8d58238b4f878bab af0a167573e97ce681c521 Backdoor.Linux.BASHLITE.SMJC 23a704d6677e77308d763d03340adf2321e547007 b98e424933aec3cb456ea61 Backdoor.Linux.BASHLITE.SMJC 267600324455dcs01305e67920a0431c31b1218ee b30639521b350c9a6968b8 Backdoor.Linux.BASHLITE.SMJC 46589461d1a2c2cda790032d5e7bd4c1b9f3a68113 915985abe11a7d6c477d6 Backdoor.Linux.BASHLITE.SMJC 47d5822c294a246e01arcc00019595d2b7ab8625 20b5c2c6d60c7b14c29f698ff7e4566d9b9b86778 Backdoor.Linux.BASHLITE.SMJC 556286f0de7b14259f698ff7e4566d9b9b86778 556286f0de7b14c521d5e6a1 Backdoor.Linux.BASHLITE.SMJC 83a1133d980a581d8207c 6888a5d35be8fbbdab5ef3tbe9afc6ac6d9866028cc 37258b60tbc5r9c3c58f 9252295167d244654b03bba9rc4e2c829ba599465 4226434b01b91a5erc361949 e6226632c653bdace9115b1a5erc361949 e7268a2ec167d24654b03bba9rc4e2c829ba599465 428448501b91a5erc361949 4264364156170482658166703058321831 ec67007ra342c90517d11c e7970867a8c446561a665da3851f670505477a4feb 6363676b7dba822ed95b637968203b68759e73a eddd904455e94a4582b493 Backdoor.Linux.MIRALVWIUP 060b29eea4d15170b4398 18911136672325b494af13105081668eb916589ad 55628660c4764488077419b96 Backdoor.Linux.MIRALVWIUP 060b29eea4d15170b4047642725db5 1994a73258494451870b4047e47275db5 Backdoor.Linux.MIRALVWIUP 060b29ee325454a4939	04f403398c8a10d2d7a87	
af0a167573e976c681c521 Backdoor.Linux.BASHLITE.SMJC 23a70da6677e77308d763d03340adf2321e547007 Backdoor.Linux.BASHLITE.SMJC 267600324455drc91f395e87920a0431c31b1218ee Backdoor.Linux.BASHLITE.SMJC 3b639521b350c3e6968b8 H6589461d1a2c2cda790032d5e7bd4c1b9f3a68113 915/985abe11a7d6c4f7d6 H745882c2e94a246e01afcc0d01f9595d2b7ab8625 2b65c26d6d0e7bf45e9876 Backdoor.Linux.BASHLITE.SMJC Sa4d5a606ce47671te29f698ff7e4566d9b9b86778 Backdoor.Linux.BASHLITE.SMJC 08ba612006831325d7921e 555286fde73600253f00cf10ece18c3840377c72419 e6ac2690116ee25898b9 E622c630c503bdace9116ec521d566a1 83c1183d980a581d8207c G888a5d35be8fbbdab5ef3fbe93afc6ac5d9866028cc 37258b60fbc5c79c3c58f 992629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd58f9 a12ea10f700B8004ee9c097[2a17e9edc3c2251d2 5ef658ab176197se07ce a364513adc7103059ee20580d8014369bc3321831 ec567b0f7342c9b517d12c c567b0f7342c9b517d12c c97d08c7a8c4465e1d6ef5da385ff670505477a4feb Backdoor.Linux.MIRAI.VWIUP 060b29eead55170b39e8 1630376620368759e73a ed6q004455e94a458e2b493 1630376620366759652383 163113e7c325b494af1305081668eb916589daf 5c1962130ec2c13095b637945236 163113e7c325b494af1305081668e	232bd7a7beada597ce71f1607a8d58238b4f878bab	
23a70da6677677308d763d03340adf2321e547007 Backdoor.Linux.BASHLITE.SMJC b98e424933acc3cb456cea61 Backdoor.Linux.BASHLITE.SMJC 267600324455dcc91f395687920a0431c31b1218ee Backdoor.Linux.BASHLITE.SMJC b36839521b350c9a6968b8 46589461d122c0dr790032d5e7bd4c1b9f3a68113 Backdoor.Linux.BASHLITE.SMJC b15985abe1fa7d6c477d6 47d582c2e94a246e01afcc0d01f9595d2b7ab8c25 2b05c26d60467b45e9876 Backdoor.Linux.BASHLITE.SMJC 55c286fdef36002537006110eca18c3840377c72419 E6ac2690116ee589e8be9 E55c286fdef36002537006110eca18c3840377c72419 E6ac2690116ee589e8be9 6226c32ec5b3bdace911cec2c14676fbf4c51d5e6a1 83c1183d980a581d8207c E8885d35be8bbdab5ef3fbe9afc6ac6d9866028cc 37258be0hot5c79e3c368f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b43801f9113e7cd5f9f9 37258be0hot5c79e3c368f 364513ac7103c95ee205580d8014369bc3221831 E667b0177342c9b517d1cc 67008c7a8c4455e1deef5da385ff670505477a4feb 364513ac7103c95ee205580d8014369bc321831 E667b017a342c9b517d1cc 8ackdoor.Linux.MIRAI.VWIUP 060b29eea4d15170b4398 19307442c9b516316ccd700 060b29eea4d15170b4398 E8ckdoor.Linux.MIRAI.VWIUP 1906ea3cc4d1687674177ab25ed590b0c3a9b7 1904ea37c230546274174258226950a7419b96 1904e37c243055846788 1904c37c258c2451248362693 1904c37c258c2451248362693 1904c37c258c24512436226050b0c3a9b7 1904c37c258c24526580b0c328b	af0a167573e976c681c521	
b98e424933aec3cb456ea61 Backdoor.Linux.BASHLITE.SMJC 267600324455drc91r395687920a0431c31b1218ee Backdoor.Linux.BASHLITE.SMJC b3639521b350c3e8058b8 Holdsepart 46589461d1a2c2cda790032d5e7bd4c1b9f3a68113 Backdoor.Linux.BASHLITE.SMJC 915/985abe1fa7d6c4f7d6 Holdsepart 4f05e82c2e94a246e01afcc0d01f9595d2b7ab8625 Backdoor.Linux.BASHLITE.SMJC 2b05c26d6d0e7bf45e9876 Backdoor.Linux.BASHLITE.SMJC 552286fcef360022530006f10eca18c3840377c72419 Backdoor.Linux.BASHLITE.SMJC 662c900116ee5898be9 Ge226c32ec5b3tdace911cec2c14676fbf4c51d5e6a1 831183d980a581d8207c B888a61205 6888a5d5be8fbtadbsef3fbe9afc6ac6d9866028cc Backdoor.Linux.BASHLITE.SMJC 37258b60fbc5c79c3c58f Bbc229b167024654b03bba97c4e2c829ba599465 9b2629e5167d24654b03bba97c4e2c829ba599465 Holdset87103056e20580d8014369bc3321831 ec667b0f7a342e9b517d1cc C97008c7a8c4465e1d6ef5da385ff670505477a4feb 0a37 6230e3100da5e687a Backdoor.Linux.MIRALVWIUP Gob02eea4d15170b4398 Backdoor.Linux.MIRALVWIUP 060b2eea4d15170b4398 Backdoor.Linux.MIRALVWIUP 060b2eea4d15170b4398 Backdoor.Linux.MIRALVWIUP 1536483592451a49a922a004dc7e48807741	23a70da6677e77308d763d03340adf2321e547007	
267600324455dcc91f395e87920a0431c31b1218ee Backdoor.Linux.BASHLITE.SMJC b3b639521b305c9a698b8 46589461d1a2c2cdr790032d5e7b44c1b9f3a68113 915f985abe1fa706c4f7d6 4fd5e82c2e94a246e01afcc0d01f9595d2b7ab8625 205c2c2d6d0erbf45e9876 564d5a606ce477671e29f698ff7e4566d9b9b86778 08ba612006833521b7921e 5556286fdef3600253f006f10eca18c3840377c72419 6622603016ee589e8be9 622c6:32c5b3bdace911oec214676fbf4c51d5e6a1 83c1183d980a581d8207c 6888a5d35be8b10ab5ef3fbe9afc6ac6d9866028cc 37288b60fbc5c79c3c58f 9b26229e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f99 af2zeac107700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee 3634513adc7103c95e20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c c 97d08c7a8c4465e1deef5da385ff670505477a4feb 0a37623002d1878d426094bdf6e355383 3f3319bbb4d7da0725db5 f4ffa1041d89852588c1952fd7d4c82cf581c6cd70 060c29eea4d15170b4398 8ackdoor.Linux.MIRAI.VWIUP 060c29eea4d15170b4398 1535e8359c2451a49a922a004dc7e488077419b96 56796273862420542680230637451741 17445efaaeb3cc7bde7 159efac31317851/04a9ff3d3df914191cf15d171 7445efaaeb3cc7bd7 159efac314137851/04a9ff3d3df914191cf15d171 7445efaaeb3cc7bd7 56796273862745286788	b98e424933aec3cb456ea61	
b3b639521b350c9a6968b8 46589461d1a2c2cda790032d5e7b44c1b9f3a68113 44658242c2ed4246e01afcc0d01f9595d2b7ab8625 2005c266d0c97b45e9876 5a4d5a606cc47671c29f698f7c45566d9b9b86778 08ba61200683325d7921e 556286fdef3600253f006f10eca18c3840377c72419 66ac2690116ee589e8be9 62ac2630116ee589e8be9 6226c32ec5b3bdace911cec2C14676fbf4c51d5e6a1 83c1183d980a581d8207c 6888a5d35be87bbdab5ef3bdab97c4e2c829ba599465 42b843801f9b13a7cd5f99 42b843801f9b13a7cd5f99 af2ce610f70018d004ce9c097f2a17e9edc3c2251d2 5ef58abf761976a97c5e af364513adc7103c95ee20580d8014369bc3321831 ccf67b0f7a342c9b517d1cc c97d08c7a8c4465e1def5da385ff670505477a4feb 0376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45821493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f3319bb4dd7da0725db5 f44f#a1041088952588c1952f07dc4c82cf581c6cd70 060b29eea4d15170b4398 fs9ear3137851/04287235b494af13d5081668e916589daf 5cf92cf1302cf3a922004dc7e488077419b96 c7962c73825b494af13d5d9141491cf15d171 744a5efaaeb3cc7bde7 159efac3813137851/040a9ff33df914191cf15d171 7445efaaeb3cc7bde7 159efac3813137851/040a9ff33df914191cf15d371 7445efaaeb3cc7bde7 159efac3813137851/040a9ff33df914191cf15d371 7445455846488	267600324455dcc91f395e87920a0431c31b1218ee	Backdoor.Linux.BASHLITE.SMJC
46589461d1a2c2cda790032d5e7bd4c1b9f3a68113 9157985abe1fa7d6c4f7d6 44f5e82c2c2e942246e01afcc0001f9595d2b7ab8625 2b05c26d6d0e7bf45e9876 5a4d5a6056cv26942246e01afcc0001f9595d2b7ab8625 2b05c26d6d0e7bf45e9876 5a4d5a6056cv26942246e01afcc0001f9595d2b7ab8625 2b05c26d6d0e7bf45e9876 556286fcdef3600253f006f10eca18c3840377c72419 e6ac2690116ec889e8be9 662c652b3tdace75b3tdace911cec2c14676fbf4c51d5e6a1 83c1183d980a581d8207c 6888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc 37258b60hc5c7.9c.3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f9f9 af2ceac107700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e87a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02a7878d426094bdfe355383 3f319bb4dd7da0725db5 f891113e672325b494af13f05081668eb916589daf 5c9620545a4a9822c004dc7e488077419b96 c7b9da87822768e22df236 159efac3fa13178f51f0da9ff13d3f914191cf15d171	b3b639521b350c9a6968b8	
915f985abe1fa7d6c4f7d6 4fd5e82c2e94a246e01afcc0d01f9595d2b7ab8625 2b05c26d6d07fxf45e9876 5a4d5a6066c47671e29f698ff7e4566d9b9b86778 08ba61200683f325d7921e 556286fde67b7d5200253006f10eca18c3840377c72419 e6ac2690116ee589e8be9 6226c32ec5b3bdace911cec2c14676fbf4c51d5e6a1 33c1183090a581d8207c 6888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc 37288b60fbc5c792.3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f99 af2ee107700b8004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1def5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a906f0d02af878d426094bdf6e355383 3f5319bb4dd7da0725db5 f891113e672325b494af13f05081668eb916589daf 5cf9627130e2cf3a925b494 f891113e672325b494af13f05081668eb916589daf cf99c2130e2cf3a95cbe9 153efea359e2451a49a922a004dc7e488077419b96 c7byda87822768e22df2236 159efac341317851f0da9ff13d3d914191cf15d171 f74a5efa	46589461d1a2c2cda790032d5e7bd4c1b9f3a68113	
4fd5e82c2e94a246e01afcc0d01f9595d2b7ab8625 2b05c26d6d0e7bf45e9876 5a4d5a6066ce47671e29f698f7e4566d9b9b86778 08ba61200683f325d7921e 556286fdef3600253f006f10eca18c3840377c72419 e6a2c690116ee589e8be9 62226c32ec5b3bdace911cec2c14676fbf4c51d5e6a1 33c1183d980a581d8207c 6888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc 37258b60fbc5c79c3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b1ae7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0904455e94a45882b493 fd708735a59b06f0d02af878d426094bdf6e355383 3f5319bb4d7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 060b29eea4d15170b4398 f891113acf7322b494af13f05081668eb916589daf 5cr962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7/445efaeb3c7bde7 190dee3fcc4d16b87674177ab25ed590b0c3a9b7 190dee3fc	915f985abe1fa7d6c4f7d6	
2b05c26d6d0e7bf45e9876	4fd5e82c2e94a246e01afcc0d01f9595d2b7ab8625	
5a4d5a6066ce47671e29f698ff7e4566d9b9b86778 08ba61200683i325d7921e 556286fcde3600253006f10eca18c3840377c72419 e6ac2690116ee589e8be9 6226032ec5b3bdace911cec2c14676fbf4c51d5e6a1 33c1183d980a581d8207c 6888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc 37258b60fbc5c79c3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c44d5e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 060b29eea4d1517014398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7/445efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 15454a97258d314558a678a	2b05c26d6d0e7bf45e9876	
08ba61200683f325d7921e 556286fdef3600253f006f10eca18c3840377c72419 e6ac2690116ee589e8be9 6226c32ec5b3bdace911cec2c14676fbf4c51d5e6a1 83c1183d980a581d8207c 6888a5d35be8tbbdab5ef3fbe9afc6ac6d9866028cc 7258b60fbc5c79c3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7db822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 060b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22d12236 159efac3fa13178f51f0da9fff3d3d914191cf15d171 f744s5eaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 190dee3fc4dd16b87678a	5a4d5a6066ce47671e29f698ff7e4566d9b9b86778	
556286fdef36002537006f10eca18c3840377c72419 e6ac2690116ee589e8be9 6226c32ec5b3bdace911cec2c14676fbf4c51d5e6a1 33c1183d980a581d8207c 6888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc 37258b60fbc5c79c3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 060b29eead415170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7/4a5faaeb3c7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d3144558a678a	08ba61200683f325d7921e	
e6ac2690116ee589e8be9 6226c32ec5b3bdace911cec2c14676fbf4c51d5e6a1 33c1183d980a581d8207c 68888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc 37258b60fbc5c79c3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7db822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 060b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7/Ha5efaaeb3c7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d3144558a678a	556286fdef3600253f006f10eca18c3840377c72419	
6226c32ec5b3bbace911cec2c14676fbf4c51d5e6a1 83c1183d980a581d8207c 6888a5d35be8fbbdab5e3fbe9afc6ac6d9866028cc 37258b60fbc5c79c3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bb4dd7da0725db5 fd44fa1041d89852588c1952fd7d4c82cf581c6cd70 060b29eea4d15170b4398 f891113e672325b494af1305081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f44sefaaeb3c7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	e6ac2690116ee589e8be9	
83c1183d980a581d8207c 6888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc 37258b60fbc5c79c3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ce20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 af5131bbb4dd7da0725db5 fd4ffa1041d89852588c1952fd7dc82cf581c6cd70 060b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7/H45efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7	6226c32ec5b3bdace911cec2c14676fbf4c51d5e6a1	
6888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc 37258b60fbc5c79c3c58f 9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 5ef658abf7619763c465816670505477a4feb 0a376230e3100da5e687a 6ed904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 60b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 5cb962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 5b9da87822768e22df2236 159dea37a1317851f0da9fff3d3df914191cf15d171 7f4456faeb3c7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 156f4a9a	83c1183d980a581d8207c	
37258b60fbc5c79c3c58f	6888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc	
9b2629e5167d24654b03bba97c4e2c829ba599465 42b843801f9b13e7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 06b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 1599fac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	37258b60fbc5c79c3c58f	
42b843801f9b13e7cd5f9f9 af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a a6d904455e94a4582b493 de3d0a766b7dba822ed95b637968203b68759e73a aed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 af5319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 backdoor.Linux.MIRAI.VWIUP 060b29eea4d15170b4398 backdoor.Linux.MIRAI.VWIUP f891113e672325b494af13f05081668eb916589daf backdoor.Linux.MIRAI.VWIUP 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 15a9efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	9b2629e5167d24654b03bba97c4e2c829ba599465	
af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2 5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 060b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	42b843801f9b13e7cd5f9f9	
5ef658abf761975e07cee a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a a364513adc7103c95ee20580d80159e73a de3d0a766b7dba822ed95b637968203b68759e73a a6d60904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 Backdoor.Linux.MIRAI.VWIUP 060b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 seckdoor.2004dc7e488077419b96 153ef8359e2451a49a922a004dc7e488077419b96 seckdoor.4007 7b9da87822768e22df2236 seckdoor.4007 159efac3fa13178f51f0da9fff3d3df914191cf15d171 seckdoor.4007 7f4a5efaaeb3cc7bde7 seckdoor.2004dc7e488077419b96 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	af2eae10f700b8d004ce9c097f2a17e9edc3c2251d2	
a364513adc7103c95ee20580d8014369bc3321831 ec567b0f7a342c9b517d1cc c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 06b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	5ef658abf761975e07cee	
ec567b0f7a342c9b517d1cc	a364513adc7103c95ee20580d8014369bc3321831	
c97d08c7a8c4465e1d6ef5da385ff670505477a4feb 0a376230e3100da5e687a de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 060b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	ec567b0f7a342c9b517d1cc	
0a376230e3100da5e687a	c97d08c7a8c4465e1d6ef5da385ff670505477a4feb	
de3d0a766b7dba822ed95b637968203b68759e73a ed6d904455e94a45882b493 fd70873b5a9b06f0d02af878d426094bdf6e355383 3f5319bbb4dd7da0725db5 f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 06b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	0a376230e3100da5e687a	
ed6d904455e94a45882b493 Image: Content of the system o	de3d0a766b7dba822ed95b637968203b68759e73a	
fd70873b5a9b06f0d02af878d426094bdf6e355383 Backdoor.Linux.MIRAI.VWIUP f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 Backdoor.Linux.MIRAI.VWIUP 060b29eea4d15170b4398 Backdoor.Linux.MIRAI.VWIUP f891113e672325b494af13f05081668eb916589daf Scf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 Sc7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 Tf4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 Sd5f4a9a7258d314558a678a	ed6d904455e94a45882b493	
3f5319bbb4dd7da0725db5 Backdoor.Linux.MIRAI.VWIUP f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 Backdoor.Linux.MIRAI.VWIUP 060b29eea4d15170b4398 Backdoor.Linux.MIRAI.VWIUP f891113e672325b494af13f05081668eb916589daf Scf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 Sc7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 Tf4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 Sd54a9a7258d314558a678a	fd70873b5a9b06f0d02af878d426094bdf6e355383	
f44ffa1041d89852588c1952fd7d4c82cf581c6cd70 Backdoor.Linux.MIRAL.WIOP 060b29eea4d15170b4398 Backdoor.Linux.MIRAL.WIOP f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 5c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	3f5319bbb4dd7da0725db5	
060b29eea4d15170b4398 f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	f44ffa1041d89852588c1952fd7d4c82cf581c6cd70	Backdoor.Linux.MIRAI.VWIUP
f891113e672325b494af13f05081668eb916589daf 5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	060b29eea4d15170b4398	
5cf962f130e2cf3a95cbe9 15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a 159efac3fa13178f51f0da9fff3d3df914191cf15d171	f891113e672325b494af13f05081668eb916589daf	
15a5e8359e2451a49a922a004dc7e488077419b96 c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	5cf962f130e2cf3a95cbe9	
c7b9da87822768e22df2236 159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	15a5e8359e2451a49a922a004dc7e488077419b96	
159efac3fa13178f51f0da9fff3d3df914191cf15d171 7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	c7b9da87822768e22df2236	
7f4a5efaaeb3cc7bde7 190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	159efac3fa13178f51f0da9fff3d3df914191cf15d171	
190dee3fcc4dd16b87674177ab25ed590b0c3a9b7 d5f4a9a7258d314558a678a	7f4a5efaaeb3cc7bde7	
d5f4a9a7258d314558a678a	190dee3fcc4dd16b87674177ab25ed590b0c3a9b7	
	d5f4a9a7258d314558a678a	

[TLP:CLEAR, ID:202410081500, Page 9 of 14]



HC3: Analyst Note



October 8, 2024 TLP:CLEAR Report: 202410081500

Trend Micro IOCs				
22e925219f1b8db8f81809abf8c904ca52ee9f78b88 e2d1a03872db465670b06				
7d253e84fea4349307177aced6dc3c1b20cc96239cf				
2ff2274cb0bd52ae5a77d				
ad683393be8c09609588c67b9b978294b01fe04fa4	sora arm5			
dbca92eba8b360792361ec	3018.81113			
dda2e6e5599a2e16dc0f0fce5579992a841063f1a7				
1b7da9444aa92585f46245				
4c926ee55c6e3d1f881080c4b61734f3e7cf96124d 8cb2c1fe33c8e8d8754a04	sora.arm5			
41f90b23dbc330f586c0bf5c6643d00fbd8e215d12	sora arm5			
22c1f156390a1d93d7d853	sola.ams			
489fc54886d20e31c9e9e099712bfb85e63ae1633a	sora arm5			
17840a956f0b1f6559621d				
616ca0c082553a61f8fda6a248129dc540ff51561b4	sora.arm5	Trojan.Linux.MIRAI.SMNM1		
495041951135b1c605788				
/12/c35dc0e8edc31bba08dda48/dd496b82d5960				
5400361060aatac4ec0023a				
811eb98et2ed4d99c6aUd4818b6ae17b4bc137taUet				
000000000000000000000000000000000000000				
98880000000000000000000000000000000000				
120eu9ee02131u01171430		•		
ch1c494chbf1fc8707f942	sora.arm5			
0423e9059fe3a60c889c9dbf0a91e2a68671f5e19d		•		
a17b03804666569c7e1697				
45bce22f91e2116f2334fe9899fbf6f157847ddd840				
688f12498ec53b8dfeb5e		Backdoor.Linux.MIRAI.SMNM4		
687f1969da1747f27a315878560fa15d99f15176e8				
b045255e1318e2d9b2d30f		Backuoor.Linux.WIRAI.VWIOO		
355d6ccef10ded805ab247c49dffd9e316608f7a4e0				
1e4b9020a04066b9d7c17		Backdoor Linux MIRALSMMR1		
815e9af39e5e143f81f4b043c17931a055bf31f852a				
d91fa6627140c0370c868				
ecc1e3f8332de94d830ed97cd07867b90a405bc9cc	sora.sh4			
108deccec51badb4a2707c				
e71aca778ea1753973023e6aa29014451930c15e53	sora.x86			
107000010002000000004				
2626df0do740405o45751	sora.mpsl			
201/chad52/ddp21/ab3df11c58021d8030910bf7pa07		•		
6/5e70780c2dbd66f7e90b	sora.m68k			
3f8e65988b8e2909f0ea5605f655348efb87565566		•		
808c29d136001239b7dfa9	sora.mips	Backdoor.Linux.MIRAI.VWIUQ		
43cb46b7e87317899a80134eb107597c4e80aed15				
0b52606565c4aa9928d5ca0				
55c4675a84c1ee40e67209dfde25a5d1c1979454ec	coro orme	1		
2120047026d94f64d57744	5018.811110			
64608b5a68867aaa21574cd11b7008c946c026dbf4		1		
3c2096280e4ee033da5819				
0ca27c002e3f905dddf9083c9b2f8b3c0ba8fb0976c	sora ppc			
6a06180f623c6acc6d8ca	Sola.ppc			





Defense and Mitigations

On their website, F5 provides guidance on what to consider if you think the security of your BIG-IP system has been compromised, and provides recommendations depending on your corporate security policy.

If you suspect that your BIG-IP system is compromised, immediately notify the group in your organization that handles such incidents (typically IT). Proceed according to either an existing, defined process or policy, or using the group's recommendation.

Your internal process or policy dictates the specific actions that are relevant to your environment and may include an immediate action, such as the following:

- Isolating the compromised box from the rest of your network.
- Removing the malware by way of a clean install of the system.
- Recovering the configuration with a backup that is not infected and does not include a configuration that allows reinfection.
- Investigating the root cause of the security vulnerability.

The following list provides common indicators of security being compromised, though the list is not comprehensive:

- On platforms with a Trusted Platform Module (TPM), one indicator is that the Platform Configuration Register (PCR) values do not match the values published by F5. For more information about comparing PCR and published F5 values, refer to the following articles:
 - For BIG-IP 14.1.0 and later, refer to K58311205: Overview of Local Attestation and Remote Attestation with TPM on the BIG-IP system.
 - For versions prior to BIG-IP 14.1.0 and cases when the local or remote attestation test results are Unavailable or Invalid, refer to K93302141: Performing manual attestation with TPM on BIG-IP systems.
- Typically, when you upgrade BIG-IP software, the PCR values change. After the upgrade, you verify your BIOS version and then compare the values. For more information about verifying your BIOS version, refer to K14212: Displaying BIOS version information for BIG-IP systems (11.x).
- The BIG-IP system runs unknown processes.
- There are large spikes in device-generated traffic, which is typically an indication that the device is part of a botnet.
- There are unknown entries in /etc/init.d. When shut down, they may be used to ensure a malicious process is restarted.
- There are additions to various cron files; for example, the root user crontab is not updated.
 - You can check the system crontabs by looking at the file modification times for the cron files in /etc. For example: Is -It /etc/cron*
 - You can check the root user crontab by looking at the file modification time for /var/spool/cron/root. For example: Is -It /var/spool/cron/root
- There is an outbound connection to an unauthorized server, which you can see by running the lsof command.
- There are files or processes running from the /boot/ or /tmp/ directories.
- New files are created in unexpected directories such as /usr/local/www.
- New hidden files are created with unexpected, random, filenames. Note that any Unix filename





HC3: Analyst Note

October 8, 2024 TLP:CLEAR Report: 202410081500

beginning with a period (.) indicates a hidden file.

- $\circ~$ You can search for hidden files using the find command. For example: find /usr/local/www type f -name '.*'
- Unexpected log entries (for example, 'File does not exist' errors) in /var/log/httpd/httpd_errors may indicate reconnaissance or attempts to exploit a system, but they do not necessarily indicate successful exploitation.
 - In BIG-IP 14.1.0 and later, you can find these log entries running journalctl /bin/logger. Note that the systemd journal is limited to 20MB and therefore may quickly rotate log entries.

The majority of compromised security is a result of one or both of the following issues:

- There are management or self IP administrative ports accessible to the internet because either the management or self IP is public (and port 443 is open), or because traffic is rerouted to it by way of network address translation (NAT).
- You are using weak or default passwords.

Recovery

To recover the system, consider the following recommendations:

- Important: F5 strongly recommends that you consult your corporate security policy for guidelines about incident handling procedures that are specific to your organization. More specifically, review the policies to ensure that they comply with evidence collection procedures for a security incident before you attempt to recover the system.
- Perform a clean installation of the system. For more information, refer to <u>K13117: Performing a</u> <u>clean installation of BIG-IP 11.x 17.x.</u>
- Perform a clean installation and restore the configuration from a user configuration set (UCS) file made before the security was compromised. For more information, refer to <u>K13132: Backing up</u> and restoring BIG-IP configuration files with a UCS archive.
- Take steps to secure the system and prevent the clean installation from becoming compromised.
- If you do not have a UCS file made before the security was compromised, then seriously consider rebuilding the configuration from scratch.
- All security keys, certificates and credentials that are installed on the system may be compromised, and it may be prudent to assume that they are. Regenerate those in accordance with your corporate security policy.
- On platforms with a TPM, if the PCR values do not match the F5-published values, and you confirm it is not due to a false positive, open a case with F5 Support.
 - For more information, refer to <u>K2633: Instructions for submitting a support case to F5.</u>
 - $\circ~$ If you confirm tampering by an attacker by examining the PCR values, engage F5 Consulting Services or the F5 Sales team to replace the hardware.

The Way Forward

In addition to the aforementioned defense and mitigation strategies and recommendations, HC3 recommends that HPH organizations utilize resources from <u>CISA Stop Ransomware</u>, <u>HHS 405(d)</u>, and the <u>H-ISAC</u> to proactively and reactively aid healthcare organizations with cybersecurity awareness and guidance.





The probability of cyber threat actors targeting any industry remains high, but especially so for the Healthcare and Public Health (HPH) sector. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with the tools and resources necessary to prevent a cyberattack remains the best way forward for healthcare organizations.

Relevant HHS Reports

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

<u>HC3: Sector Alert - Russian State-Sponsored and Criminal Cryber Threats to Critical Infrastructure</u> (April 26, 2022)

<u>HC3: Sector Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical</u> <u>Infrastructure</u> (January 11, 2022)

HC3: Threat Briefing – Iranian Threat Actors & Healthcare (November 3, 2022)

HC3: Threat Briefing – North Korean and Chinese Cyber Crime Threats to the HPH (September 21, 2023)

HC3: Threat Briefing – Russian Threat Actors Targeting the HPH Sector (February 15, 2024)

HC3: Threat Profile - China-Based Threat Actors (August 16, 2023)

<u>Health-ISAC and HC3 Joint Bulletin - Potential Malicious Cyber Attacks from Russia - Credible Threats to US</u> <u>Critical Infrastructure Sectors</u> (March 22, 2022)

References

"12 Vulnerabilities of Christmas- CVE -2020-5902." Orpheus. December 8, 2020. <u>https://orpheus-cyber.com/12-vulnerabilities-of-christmas-cve-2020-5902/?lang=en</u>

Cipollone, Francesco. "F5's Big IP CVE-2023-46747 Critical Security Flaw: A Deep Dive into CVE-2023-46747 and Its Exploit Chain." Phoenix Security. November 3, 2023. <u>https://phoenix.security/f5-critical-cve-2023-46747/</u>

"CVE-2020-5902 Detail." National Vulnerability Database. July 1, 2020. <u>https://nvd.nist.gov/vuln/detail/cve-2020-5902</u>

"CVE-2022-1388 Detail." National Vulnerability Database. May 5, 2022. <u>https://nvd.nist.gov/vuln/detail/CVE-2022-1388</u>

"CVE-2023-46747 Detail." National Vulnerability Database. October 26, 2023. https://nvd.nist.gov/vuln/detail/CVE-2023-46747

"CVE-2023-46748 Detail." National Vulnerability Database. October 26, 2023. https://nvd.nist.gov/vuln/detail/CVE-2023-46748

Greig, Jonathan. "Chinese government hacker exploiting ScreenConnect, F5 bugs to attack defense and

[TLP:CLEAR, ID:202410081500, Page 13 of 14]





government entities." The Record. March 21, 2024. <u>https://therecord.media/chinese-government-hacker-exploiting-bugs-to-target-defense-government-sectors</u>

"K11438344: Considerations and guidance when you suspect a security compromise on a BIG-IP system." F5. Updated July 26, 2024. <u>https://my.f5.com/manage/s/article/K11438344</u>

Malhotra, Asheer. "Threat Advisory: Critical F5 BIG-IP Vulnerability." Cisco Talos Blog. May 10, 2022. <u>https://blog.talosintelligence.com/threat-advisory-critical-f5-big-ip-vuln/</u>

Orleans, Alex. "Who Is PIONEER KITTEN?" CrowdStrike. August 31, 2020. https://www.crowdstrike.com/blog/who-is-pioneer-kitten/

Ozeren, Sila. "Pioneer Kitten: Iranian Threat Actors Facilitate Ransomware Attacks Against U.S. Organizations." Picus Security. August 28, 2024. <u>https://www.picussecurity.com/resource/blog/pioneer-kitten-cisa-alert-aa24-241a</u>

Raggi, Michael and Adam Aprahamian, Dan Kelly, Mathew Potaczek, Marcin Siedlarz, Austin Larsen. "Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect." Mandiant. March 21, 2024. <u>https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect</u>

"Recent vulnerabilities in F5 BIG-IP devices exploited by threat actors." Field Effect. November 2, 2023. <u>https://fieldeffect.com/blog/vulnerabilities-f5-big-ip-devices-exploited</u>

"Threat Brief: CVE-2022-1388." Unit 42. May 10, 2022. <u>https://unit42.paloaltonetworks.com/cve-2022-1388/</u>

"UNC5174." Malpedia. Accessed September 27, 2024. https://malpedia.caad.fkie.fraunhofer.de/actor/unc5174

Contact Information

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

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