(Ex)Change of Pace: UNC2596 Observed Leveraging Vulnerabilities to Deploy Cuba Ransomware

mandiant.com/resources/unc2596-cuba-ransomware

In 2021, Mandiant observed some threat actors deploying ransomware increasingly shift to exploiting vulnerabilities as an initial infection vector. UNC2596, a threat actor that deploys COLDDRAW ransomware, publicly known as Cuba Ransomware, exemplifies this trend. While public reporting has highlighted CHANITOR campaigns as precursor for these ransomware incidents, Mandiant has also identified the exploitation of Microsoft Exchange vulnerabilities, including ProxyShell and ProxyLogon, as another access point leveraged by UNC2596 likely as early as August 2021. The content of this blog focuses on UNC2596 activity which has led to the deployment of COLDDRAW ransomware.

UNC2596 is currently the only threat actor tracked by Mandiant that uses COLDDRAW ransomware, which may suggest it's exclusively used by the group. During intrusions, these threat actors have used webshells to load the TERMITE in-memory dropper with subsequent activity involving multiple backdoors and built-in Windows utilities. Beyond commonplace tools, like Cobalt Strike BEACON and NetSupport, UNC2596 has used novel malware, including BURNTCIGAR to disable endpoint protection, WEDGECUT to enumerate active hosts, and the BUGHATCH custom downloader. In incidents where COLDDRAW was deployed, UNC2596 used a multi-faceted extortion model where data is stolen and leaked on the group's shaming website, in addition to encryption using COLDDRAW ransomware. COLDDRAW operations have impacted dozens of organizations across more than ten countries, including those within critical infrastructure.

Victimology

The threat actors behind COLDDRAW ransomware attacks have not shied away from sensitive targets (Figure 1). Their victims include utilities providers, government agencies, and organizations that support non-profits and healthcare entities, however, we have not observed them attacking hospitals or entities that provide urgent care. Around 80% of impacted victim organizations are based in North America, but they have also impacted several countries in Europe as well as other regions (Figure 2).

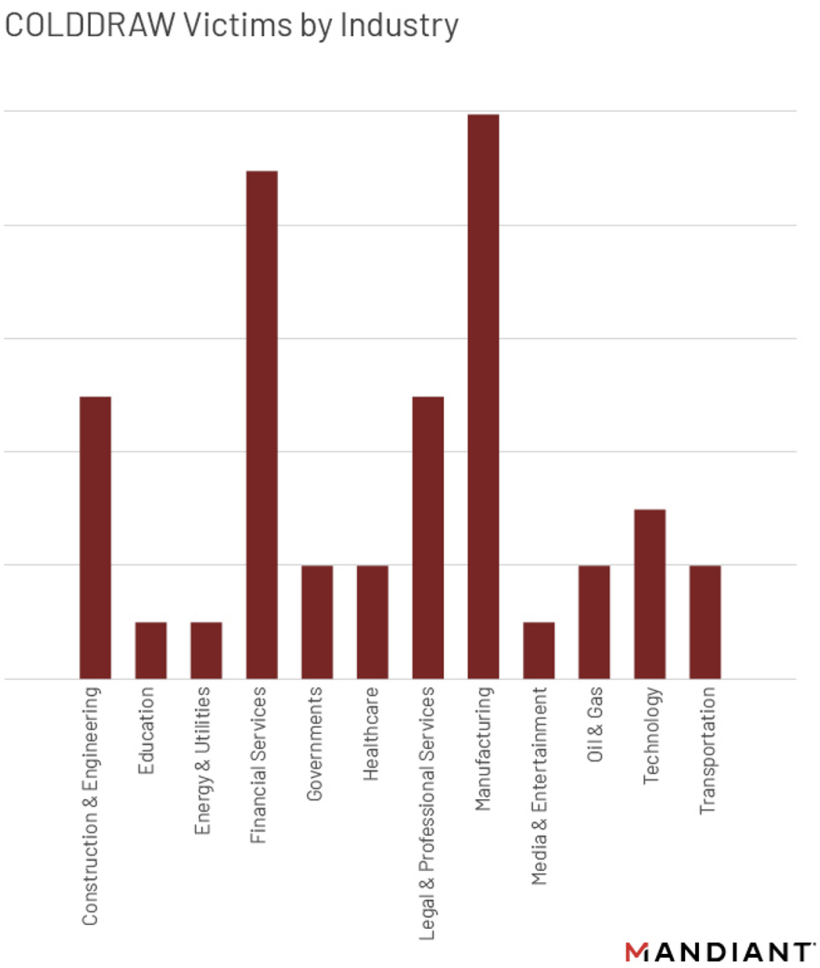

Figure 1: Alleged COLDDRAW victims by industry

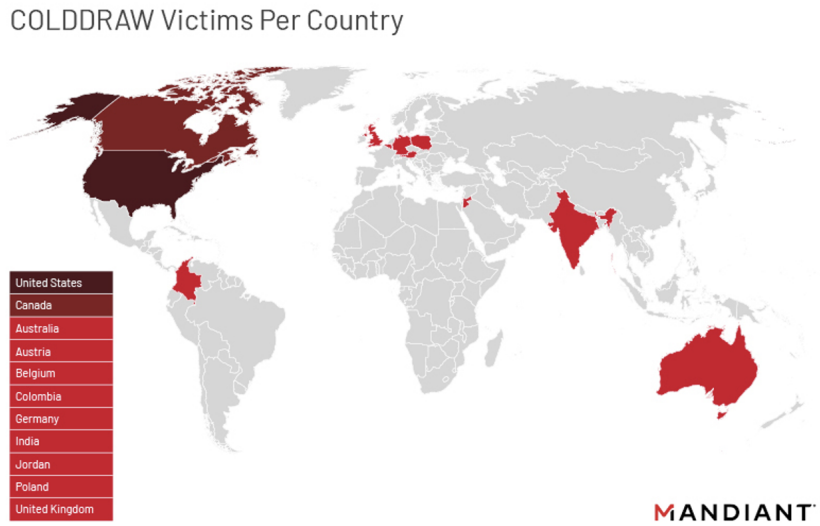

Figure 2: Alleged COLDDRAW victims by country

Shaming Website

Since at least early 2021, COLDDRAW ransomware victims have been publicly extorted by the threat actors who threaten to publish or sell stolen data (Figure 3). Each shaming post includes information on the “date the files were received.” While the shaming site was not included in ransom notes until early 2021, one of the entries on the site states that the files were received in November 2019. This is consistent with earliest samples uploaded to public malware repositories and may represent the earliest use of the ransomware. Notably, while the data associated with most of the victims listed on this site are provided for free, there is a paid section which listed only a single victim at the time of publication.

Figure 3: Cuba (aka COLDDRAW) Ransomware Shaming Tor site (2021-12-31)

Attack Lifecycle

UNC2596 incidents that have led to COLDDRAW ransomware deployment have involved a mix of public and private tools, some of which are believed to be private to them. The threat actors use several malware and utilities that are publicly available including NetSupport, Cobalt Strike BEACON, built-in Windows capabilities such as PsExec, RDP, and PowerShell, malware available for purchase such as WICKER, and exploits with publicly available proof-of-concept code. UNC2596 also uses several tools and scripts that we have not observed in use by other threat activity clusters to date, including BUGHATCH, BURNTCIGAR, WEDGECUT, and COLDDRAW. See the “Notable Malware and Tools” section for additional detail.

Initial Reconnaissance / Initial Compromise

Mandiant has observed UNC2596 frequently leverage vulnerabilities affecting public-facing Microsoft Exchange infrastructure as an initial compromise vector in recent COLDDRAW intrusions s where the initial vector was identified. The threat actors likely perform initial reconnaissance activities to identify Internet-facing systems that may be vulnerable to exploitation.

Establish Foothold

In COLDDRAW ransomware incidents, where initial access was gained via Microsoft Exchange vulnerabilities, UNC2596 subsequently deployed webshells to establish a foothold in the victim network. Mandiant has also observed these actors deploy a variety of backdoors to establish a foothold, including the publicly available NetSupport RAT, as well as BEACON and BUGHATCH, which have been deployed using the TERMITE in-memory dropper.

Escalate Privileges

COLDDRAW ransomware incidents have mainly involved the use of credentials from valid accounts to escalate privileges. In some cases, the source of these credentials is unknown, while in other cases, UNC2596 leveraged credential theft tools such as Mimikatz and WICKER. We have also observed these threat actors manipulating or creating Windows accounts and modifying file access permissions. In one intrusion, UNC2596 created a user account and added it to the administrator and RDP groups.

Internal Reconnaissance

UNC2596 has performed internal reconnaissance with the goals of identifying active network hosts that are candidates for encryption and identifying files to exfiltrate for use in their multi-faceted extortion scheme. The threat actors have used WEDGECUT, a reconnaissance tool typically with the filename *check.exe*. It identifies active hosts by sending PING requests to a list of hosts generated by a PowerShell script named *comps2.ps1* which uses the Get-ADComputer cmdlet to enumerate the Active Directory. The threat actors have interactively browsed file systems to identify files of interest. Additionally, UNC2596 has routinely used a script named *shar.bat* to map all drives to network shares, which may assist in user file discovery (Figure 4).

Figure 4: UNC2596 used a batch script to enable sharing of all drives to facilitate encryption and data harvesting

```
net share C=C:\ /grant:everyone,FULL
net share D=D:\ /grant:everyone,FULL
net share E=E:\ /grant:everyone,FULL
net share F=F:\ /grant:everyone,FULL
net share G=G:\ /grant:everyone,FULL
net share H=H:\ /grant:everyone,FULL
net share I=I:\ /grant:everyone,FULL
net share J=J:\ /grant:everyone,FULL
net share L=L:\ /grant:everyone,FULL
net share K=K:\ /grant:everyone,FULL
net share M=M:\ /grant:everyone,FULL
net share X=X:\ /grant:everyone,FULL
net share Y=Y:\ /grant:everyone,FULL
net share W=W:\ /grant:everyone,FULL
net share Z=Z:\ /grant:everyone,FULL
net share V=V:\ /grant:everyone,FULL
net share O=O:\ /grant:everyone,FULL
net share P=P:\ /grant:everyone,FULL
net share Q=Q:\ /grant:everyone,FULL
net share R=R:\ /grant:everyone,FULL
net share S=S:\ /grant:everyone,FULL
net share T=T:\ /grant:everyone,FULL
```

Move Laterally/Maintain Presence

During COLDDRAW incidents, UNC2596 actors have used several methods for lateral movement including RDP, SMB, and PsExec, frequently using BEACON to facilitate this movement. Following lateral movement, the threat actors deploy various backdoors including the publicly available NetSupport RAT, as well as BEACON and BUGHATCH, which are often deployed using the TERMITE in-memory dropper. These backdoors are sometimes executed using PowerShell launchers and have in some cases used predictable filenames. For example, NetSupport-related scripts and executables observed during COLDDRAW incidents have typically used the filename *ra* or *ra<#>* whereas BUGHATCH scripts and executables have used the filename *komar* or *komar<#>*, followed by the appropriate extension.

Complete Mission

In order to complete their mission of multi-faceted extortion, the UNC2596 attempts to steal relevant user files and then identify and encrypt networked machines. To facilitate encryption, and possibly to assist with collection efforts, the threat actors have used a batch script named *shar.bat* which maps each drive to a network share (Figure 4). These newly created shares are then available for encryption by COLDDRAW. During a more recent intrusion involving COLDDRAW, UNC2596 deployed the BURNTCIGAR utility using a batch script named *av.bat*. BURNTCIGAR is a utility first observed in November 2021 which terminates processes associated with endpoint security software to allow their ransomware and other tools to execute uninhibited. UNC2596 has also been observed exfiltrating data prior to encrypting victim systems. To date, we have not observed UNC2596 using any cloud storage providers for data exfiltration; rather, they prefer to exfiltrate data to their BEACON infrastructure. The threat actors then threaten to publish data of organizations that do not pay a ransom on their shaming site (Figure 5).

Figure 5: Sample COLDDRAW Ransom Note

Good day. All your files are encrypted. For decryption contact us.

Write here cloudkey[@]cock.li

reserve admin[@]cuba-supp.com

jabber cuba_support[@]exploit.im

We also inform that your databases, ftp server and file server were downloaded by us to our servers.

If we do not receive a message from you within three days, we regard this as a refusal to negotiate.

Check our platform: <REDACTED>[.]onion/

* Do not rename encrypted files.

* Do not try to decrypt your data using third party software,

it may cause permanent data loss.

* Do not stop process of encryption, because partial encryption cannot be decrypted.

Notable Malware and Tools

In addition to the use of publicly available malware and built-in utilities, Mandiant has observed UNC2596 use malware that is believed to be private to these threat actors, such as WEDGECUT, BUGHATCH, BURNTCIGAR, and COLDDRAW, or malware that is believed to be used by a limited number of threat actors, such as TERMITE.

WEDGECUT

WEDGECUT, which has been observed with the filename *check.exe*, is a reconnaissance tool that takes an argument containing a list of hosts or IP addresses and checks whether they are online using ICMP packets. This utility's functionality is implemented using the IcmpCreateFile, IcmpSendEcho, and IcmpCloseFile APIs to send a buffer containing the string "Date Buffer". In practice, the list provided to WEDGECUT has been generated using a PowerShell script that enumerates the Active Directory using the Get-ADComputer cmdlet.

BUGHATCH

BUGHATCH is a downloader that executes arbitrary code on the compromised system downloaded from a C&C server. The code sent by the C&C server includes PE files and PowerShell scripts. BUGHATCH has been loaded in-memory by a dropper written in PowerShell or loaded by a PowerShell script from a remote URL.

BURNTCIGAR

BURNTCIGAR is a utility that terminates processes at the kernel level by exploiting an Avast driver's undocumented IOCTL code (Table 1). The malware terminates targeted processes using the function DeviceIoControl to exploit the undocumented 0x9988C094 IOCTL code of the Avast driver, which calls ZwTerminateProcess with the given process identifier. We have observed a batch script launcher that creates and starts a kernel service called aswSP_ArPot2 loading binary file C:\windows\temp*aswArPot.sys* (legitimate Avast driver with SHA256 hash 4b5229b3250c8c08b98cb710d6c056144271de099a57ae09f5d2097fc41bd4f1).

To deploy BURNTCIGAR at a victim, the actor brings their own copy of the vulnerable Avast driver and installs it at a service.

Table 1: Processes Killed by BURNTCIGAR

Executable Processes Killed by BURNTCIGAR		
SentinelHelperService.exe	iptray.exe	dsa-connect.exe
SentinelServiceHost.exe	ccSvcHst.exe	ResponseService.exe
SentinelStaticEngineScanner.exe	sepWscSvc64.exe	avp.exe
SentinelAgent.exe	SEPAgent.exe	avpsus.exe
SentinelAgentWorker.exe	ssDVAgent.exe	klnagent.exe
SentinelUI.exe	smcgui.exe	vapm.exe

SAVAdminService.exe	PAUI.exe	VsTskMgr.exe
SavService.exe	ClientManager.exe	mfemms.exe
SEDService.exe	SBPIMSvc.exe	mfeann.exe
Alsvc.exe	SBAMSvc.exe	macmnsvc.exe
SophosCleanM64.exe	VipreNis.exe	masvc.exe
SophosFS.exe	SBAMTray.exe	macompatsvc.exe
SophosFileScanner.exe	RepMgr.exe	UpdaterUI.exe
SophosHealth.exe	RepUtils.exe	mfemactl.exe
McsAgent.exe	scanhost.exe	McTray.exe
McsClient.exe	RepUx.exe	cpda.exe
SophosSafestore64.exe	PccNtMon.exe	IDAFServerHostService.exe
SophosSafestore.exe	svcGenericHost.exe	epab_svc.exe
SSPService.exe	pccntmon.exe	epam_svc.exe
swc_service.exe	HostedAgent.exe	cptrayLogic.exe
swi_service.exe	tmlisten.exe	EPWD.exe
SophosUI.exe	logWriter.exe	FSAgentService.exe
SophosNtpService.exe	ntrtscan.exe	RemediationService.exe
hmpalert.exe	TmCCSF.exe	TESvc.exe
SophosLiveQueryService.exe	TMCPMAdapter.exe	cptrayUI.exe
SophosOsquery.exe	coreServiceShell.exe	EFRService.exe
SophosFIMService.exe	coreFrameworkHost.exe	MBCloudEA.exe
swi_fc.exe	ds_monitor.exe	MBAMService.exe
SophosMTRExtension.exe	CloudEndpointService.exe	Endpoint Agent Tray.exe
sdcservice.exe	CETASvc.exe	EAServiceMonitor.exe
SophosCleanup.exe	EndpointBasecamp.exe	MsMpEng.exe
Sophos UI.exe	WSCommunicator.exe	AvastSvc.exe
SavApi.exe	dsa.exe	aswToolsSvc.exe

sfc.exe	Notifier.exe	bcc.exe
AvWrapper.exe	WRSA.exe	anet.exe
bccavsvc.exe	a.exe	aus.exe
AvastUI.exe		

COLDDRAW

COLDDRAW is the name Mandiant uses to track the ransomware observed in Cuba Ransomware operations. This ransomware appends the .cuba file extension to encrypted files. When executed, it terminates services associated with common server applications and encrypts files on the local filesystem and attached network drives using an embedded RSA key. Encrypted files are rewritten with a COLDDRAW-generated header prior to the encrypted file contents. For large files, only the beginning and end of the file will be encrypted.

TERMITE

TERMITE is a password-protected memory-only dropper which contains an encrypted shellcode payload. Observed payloads have included BEACON, METASPLOIT stager, or BUGHATCH. TERMITE requires the actor to specify the *ClearMyTracksByProcess* export and supply a password as a command line option to operate successfully (Figure 6). Mandiant suspects that TERMITE may be available to multiple groups and is not exclusively used by UNC2596.

Figure 6: TERMITE command line execution

```
Rundll32.exe c:\windows\temp\komar.dll,ClearMyTracksByProcess 11985756
```

Tracking TERMITE

During UNC2596 intrusions involving COLDDRAW, the actors load tools and malware from web accessible systems that were also typically used for BEACON. Over a period of approximately six months, Mandiant Advanced Practices tracked a TERMITE loader at hxxp://45.32.229[.]66/*new.dll* which used the password 11985756 to decode various BEACON payloads. Ongoing analysis of TERMITE payloads collected during this timeframe showed that TERMITE underwent modifications to evade detections. UNC2596 also began using the TERMITE password 11985757 in October 2021.

CHANITOR Overlaps

Mandiant has not responded to any intrusions where we have directly observed CHANITOR malware lead to COLDDRAW ransomware; however, we have identified overlaps between CHANITOR-related operations and COLDDRAW incidents. These include infrastructure overlaps, common code signing certificates, use of a shared packer, and naming similarities for domains, files, and URL paths, among others.

- The code signing certificate with the Common Name FDFWJTORFQVNXQHFAH has been used to sign COLDDRAW payloads, as well as SENDSAFE payloads distributed by CHANITOR. Mandiant has not observed the certificate used by other threat actors.
- COLDDRAW payloads and SENDSAFE payloads distributed by CHANITOR have used a shared packer that we refer to as LONGFALL. LONGFALL, which is also known as CryptOne, has been used with a variety of malware families.
- The WICKER stealer has been used in both CHANITOR-related post-exploitation activity and COLDDRAW incidents, including samples sharing the same command and control (C&C) server.
- Payloads distributed through CHANITOR and payloads identified in COLDDRAW ransomware incidents have masqueraded as the same legitimate applications including mDNSResponder and Java.
- Public reporting has also highlighted some overlaps between COLDDRAW and ZEPPELIN, another ransomware that has reportedly been distributed via CHANITOR.

Implications

As the number of vulnerabilities identified and publicly disclosed continues to increase year after year, Mandiant has also observed an increase in the use of vulnerabilities as an initial compromise vector by ransomware threat actors including utilizing both zero-day and n-day vulnerabilities in their activity; notable examples include UNC2447 and FIN11. Shifting towards vulnerabilities for initial access could offer threat actors more accurate targeting and higher success rates when compared to malicious email campaigns, which rely more on uncontrollable factors, such as victims' interacting with malicious links or documents. The rise in zero-day usage specifically could be reflective of significant funds and resources at the disposal of ransomware operators, which are being directed towards exploit research and development or the purchasing of exploits from trusted brokers. However, threat actors do not have to use zero-days to be effective. A subset of n-day vulnerabilities are often considered attractive targets for threat actors due to their impact of publicly exposed products, ability to facilitate code execution after successful exploitation, and the availability of significant technical details and/or exploit code in public venues. As the number of vulnerabilities publicly disclosed continues to rise, we anticipate threat actors, including ransomware operators, to continue to exploit vulnerabilities in their operations.

Acknowledgements

With thanks toThomas Pullen and Adrian Hernandez for technical research, and Nick Richard for technical review.

MITRE ATT&CK

Mandiant has observed COLDDRAW activity involving the following techniques in COLDDRAW intrusions:

Table 2: MITRE ATT&CK Framework

ATT&CK Tactic Category	Techniques	
Initial Access	T1190:	Exploit Public-Facing Application
Discovery	T1010:	Application Window Discovery
	T1012:	Query Registry
	T1016:	System Network Configuration Discovery
	T1018:	Remote System Discovery
	T1033:	System Owner/User Discovery
	T1057:	Process Discovery
	T1082:	System Information Discovery
	T1083:	File and Directory Discovery
	T1087:	Account Discovery
	T1518:	Software Discovery
Impact	T1486:	Data Encrypted for Impact
	T1489:	Service Stop
Collection	T1056.001:	Keylogging
	T1074.002:	Remote Data Staging
Defense Evasion	T1027:	Obfuscated Files or Information
	T1055:	Process Injection
	T1055.003:	Thread Execution Hijacking
	T1070.004:	File Deletion
	T1112:	Modify Registry
	T1134:	Access Token Manipulation
	T1134.001:	Token Impersonation/Theft
	T1140:	Deobfuscate/Decode Files or Information
	T1497.001:	System Checks
	T1553.002:	Code Signing
	T1564.003:	Hidden Window
	T1574.011:	Services Registry Permissions Weakness
	T1620:	Reflective Code Loading

Persistence	T1098:	Account Manipulation
	T1136:	Create Account
	T1136.001:	Local Account
	T1543.003:	Windows Service
Command and Control	T1071.001:	Web Protocols
	T1071.004:	DNS
	T1095:	Non-Application Layer Protocol
	T1105:	Ingress Tool Transfer
	T1573.002:	Asymmetric Cryptography
Resource Development	T1583.003:	Virtual Private Server
	T1587.003:	Digital Certificates
	T1588.003:	Code Signing Certificates
	T1608.001:	Upload Malware
	T1608.002:	Upload Tool
	T1608.003:	Install Digital Certificate
	T1608.005:	Link Target
Execution	T1053:	Scheduled Task/Job
	T1059:	Command and Scripting Interpreter
	T1059.001:	PowerShell
	T1129:	Shared Modules
	T1569.002:	Service Execution
Lateral Movement	T1021.001:	Remote Desktop Protocol
	T1021.004:	SSH
Credential Access	T1555.003:	Credentials from Web Browsers

Mandiant Security Validation

In addition to previously released Actions, the Mandiant Security Validation (Validation) Behavior Research Team (BRT) has created VHR20220223, which will also be released today, for tactics associated with UNC2596.

A102-561, Malicious File Transfer - TERMITE, Download, Variant #3

A102-560, Malicious File Transfer - TERMITE, Download, Variant #4

A102-559, Command and Control - TERMITE, DNS Query, Variant #1

A102-558, Malicious File Transfer - WEDGECUT, Download, Variant #1

A102-557, Malicious File Transfer - TERMITE, Download, Variant #2

A102-556, Malicious File Transfer - TERMITE, Download, Variant #1

A102-555, Malicious File Transfer - BURNTCIGAR, Download, Variant #4

A102-554, Malicious File Transfer - BURNTCIGAR, Download, Variant #3

A102-553, Malicious File Transfer - BURNTCIGAR, Download, Variant #2

A102-552, Malicious File Transfer - BURNTCIGAR, Download, Variant #1

A102-572, Malicious File Transfer - BUGHATCH, Download, Variant #4

A102-551, Malicious File Transfer - BUGHATCH, Download, Variant #3

A102-550, Malicious File Transfer - BUGHATCH, Download, Variant #2

A102-549, Malicious File Transfer - BUGHATCH, Download, Variant #1

A101-830 Command and Control - COLDDRAW, DNS Query

A101-831 Malicious File Transfer - COLDDRAW, Download, Variant #2

A101-832 Malicious File Transfer - COLDDRAW, Download, Variant #3

A101-833 Malicious File Transfer - COLDDRAW, Download, Variant #4

A101-834 Malicious File Transfer - COLDDRAW, Download, Variant #5

A101-835 Malicious File Transfer - COLDDRAW, Download, Variant #6

A104-800 Protected Theater - COLDDRAW, Execution

A151-079 Malicious File Transfer - COLDDRAW, Download, Variant #1

A100-308 Malicious File Transfer - CHANITOR, Download

A100-309 Command and Control - CHANITOR, Post System Info

A150-008 Command and Control - CHANITOR, Check-in and Response

A150-047 Malicious File Transfer - CHANITOR, Download, Variant #2

A150-306 Malicious File Transfer - CHANITOR, Download, Variant #1

YARA Signatures

The following YARA rules are not intended to be used on production systems or to inform blocking rules without first being validated through an organization's own internal testing processes to ensure appropriate performance and limit the risk of false positives. These rules are intended to serve as a starting point for hunting efforts to identify samples, however, they may need adjustment over time if the malware family changes.

```
rule TERMITE
{
    meta:
        author = "Mandiant"
    strings:
        $sb1 = { E8 [4] 3D 5? E3 B6 00 7? }
        $sb2 = { 6B ?? 0A [3] 83 E9 30 }
        $si1 = "VirtualAlloc" fullword
        $ss1 = "AUTO" fullword
    condition:
        (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x010B)
and all of them
}
```

```
rule FDFWJTORFQVNXQHFAH
{
    meta:
        author = "Mandiant"
        description = "Detecting packer or cert."
        md5 = "939ab3c9a4f8eab524053e5c98d39ec9"
    strings:
        $cert = "FDFWJTORFQVNXQHFAH"
        $s1 = "VLstuTmAlanc"
        $s2 = { 54 68 F5 73 20 70 00 00 00 00 00 00 BE 66 67 72 BD 68 20 63 BD 69 6E 6F C0 1F 62 65 EC 72 75 6E
FC 6D 6E 20 50 46 53 20 B9 66 64 65 }
        $s3 = "ViGuua!Gre"
        $s4 = "6seaIdFiYdA"
    condition:
        (uint16(0) == 0x5A4D) and filesize < 2MB and ( $cert or 2 of ($s*) )
}
```

Indicators

MALWARE FAMILY	Indicator
TERMITE/BEACON	irrislaha[.]com
BEACON	leptengthinete[.]com
BEACON	siagevewilin[.]com
BEACON	surnbuithe[.]com
TERMITE	64.235.39[.]82
BEACON	64.52.169[.]174
Suspect certificate	144.172.83[.]13
BEACON	190.114.254[.]116
BEACON	185.153.199[.]164
TERMITE	45.32.229[.]66
BEACON	23.227.197[.]229
Packer imphash	2322896bcde6c37bf4a87361b576de02
Packer cert CN	FDFWJTORFQVNXQHFAH
Packer cert md5	5c00466f092b19c85873848dcd472d6f

MALWARE FAMILY	MD5	SHA1	SHA256
BUGHATCH	72a60d799ae9e4f0a3443a2f96fb4896	a304497ff076348e098310f530779002a326c264	6d5ca42906c60caa7d3e0564b0
BUGHATCH	bda33efc53c202c99c1e5afb3a13b30c	e6ea0765b9a8cd255d587b92b2a80f96fab95f15	101b3147d404150b3c0c882ab8
BUGHATCH	e78ed117f74fd7441cadc3ea18814b3e	6da8a4a32a4410742f626376cbec38986d307d5a	9ab05651daf9e8bf3c84b14613c
BUGHATCH	ba83831700a73661f99d38d7505b5646	209ffbc8ba1e93167bca9b67e0ad3561c065595d	79d6b1b6b1ecb446b0f49772bf4
WEDGECUT	c47372b368c0039a9085e2ed437ec720	4f6ee84f59984ff11147bfff67ab6e40cd7c8525	c443df1ddf8fd8a47af6fbfd0b597
BURNTCIGAR	c5e3b725080712c175840c59a37a5daa	f347fa07f13c3809e4d2d390e1d16ff91f6dc959	f68cea99e6887739cd82865f9b9
BURNTCIGAR	c9d3b29e0b7662dafc6a1839ad54a6fb	d0bbbc1866062f9a772776be6b7ef135d6c5e002	4306c5d152cdd86f3506f91633e
BURNTCIGAR	9ca2579117916ded7ac8272b7b47bb98	d1ef60835127e35154a04d0c7f65beee6e790e44	aeb044d310801d546d10b24716
BURNTCIGAR (launcher)	26c09228e76764a2002ba643afeb9415	8247880a1bad73caaeed25f670fc3dad1be0954a	6ce206a1e1224e0a9d296d5fabf
TERMITE	98a2e05f4aa648b02540d2e17946da7e	e328b5e26a04a13e80e60b4a0405512c99ddb74e	811bb84e1e9f59279f844a040bf6
TERMITE	ddf2e657a89ae38f634c4a271345808b	b73763c98523e544c0ce0da7db7142f1e039c0a2	d1e14b5f02fb020db4e215cb5c3
TERMITE	95820d16da2d9c4fbb07130639be2143	0a3ac9b182d8f14d9bc368d0c923270eed29b950	a722615c2ee101cde88c7f44fb2
TERMITE	896376ce1bbca1ed73a70341896023e0	f1be87ee03a2fb59d51cb4ba1fe2ece8ddfb5192	671e049f3e2f6b7851ca4e8eed2
TERMITE	f51c4b21445a0ece50b1f920648ed726	7c88207ff1afe8674ba32bc20b597d833d8b594a	ea5de5558396f66af8382afd98f2
TERMITE	7d4307d310ad151359b025fc5a7fca1a	49cfcecd50fcfcd3961b9d3f8fa896212b7a9527	ad12f38308a85c8792f2f7e1e46a
TERMITE	b62eec21d9443f8f66b87dd92ba34e85	172f28f61a35716762169d63f207071adf21a54c	9cec82bebe1637c50877ff11de5b
TERMITE	df0e5d91d0986fde9bc02db38eef5010	922ca12c04b064b35fd01daadf5266b8a2764c32	6cd25067316f8fe013792697f2f5
TERMITE	46b977a0838f4317425df0f2e1076451	39381976485fbe4719e4585f082a5252feedbcfd	13d333d5e3c1dd6c33dfa8fc76d
TERMITE	8c4341a4bde2b6faa76405f57e00fc48	4f3a1e917f67293578b7e823bca35c4dff923386	df89d3d1f795a77eefc14f035681
TERMITE	d5679f47d22c7c0647038ce6f54352e4	d9030bdbd0cb451788eaa176a032aa83cf7604c0	728a2d5dd2bf9c707431ff68e94c
TERMITE	e77af544cc9d163d81e78b3c4da2eee5	3ead9dd8c31d8cfb6cc53e96ec37bdcfdbbcce78	7f357ab4ac225e14a6967f89f209
TERMITE	98b2fff45a9474d61c1bd71b7a60712b	3b0ec4b6ad3cf558cac6b2c6e7d8024c438cfbc5	7b2144f2b5d722a1a8a0c47a43e
TERMITE	9a0a2f1dc7686983843ee38d3cab448f	363dc3cf956ab2a7188cf0e44bffd9fba766097d	03249bf622c3ae1dbed8b14cfaa
TERMITE	fb6da2aa2aca0ce2e0af22b2c3ba2668	55b89bad1765bbf97158070fd5cbf9ea7d449e2a	1842ddc55b4bf9c71606451d404
COLDDRAW	3e96efd37777cc01cabb3401485297aa	f008e568c313b6f41406658a77313f89df07017e	bcf0f202db47ca671ed6146040
COLDDRAW	73c0f0904105b4c220c25f64506ea986	7ef1f5946b25f56a97e824602c58076e4b1c10b6	e35593fab92606448ac4cac6cd2

COLDDRAW	20a04e7fc12259dfd4172f5232ed5ccf	82f194e6baeef6eefb42f0685c49c1e6143ec850	482b160ee2e8d94fa6e4749f77e
Exchange Payload test.hta	becdcaa3a4d933c13427bb40f9c1cfbb	ee883ec4b7b7c1eba7200ee2f9f3678f67257217	6c4b57fc995a037a0d60166deac
BEACON	c0e88dee5427aae6ce628b48a6d310a7	fd4c478f1561db6a9a0d7753741486b9075986d0	44a4ce7b5d2e154ec802a67ef14
BEACON	bb2a2818e2e4514507462aadea01b3d7	8fec34209f79debcd9c03e6a3015a8e3d26336bb	6e66caaa12c3cafd1dc3f8c6305
BEACON	48f8cd5e42cdf06d5a520ab66a5ae576	0d0ac944b9c4589a998b5032d208a16e63db5817	d8df1a4d59a0382b367fd6936cc