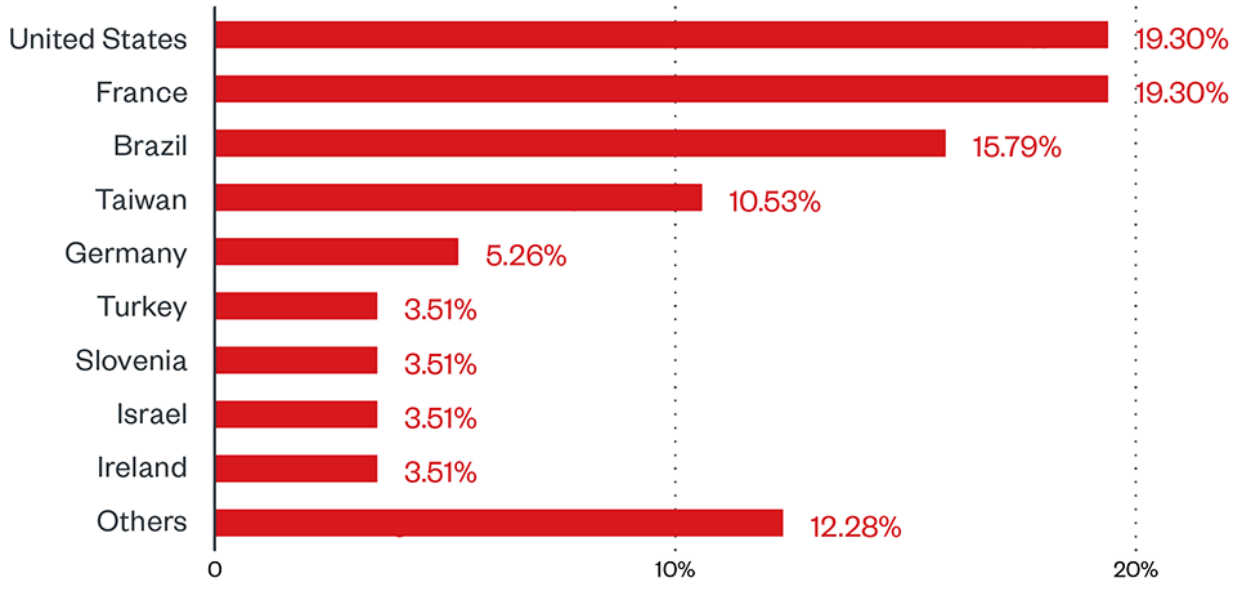
Ransomware Spotlight: RansomEXX

X

Top affected industries and countries

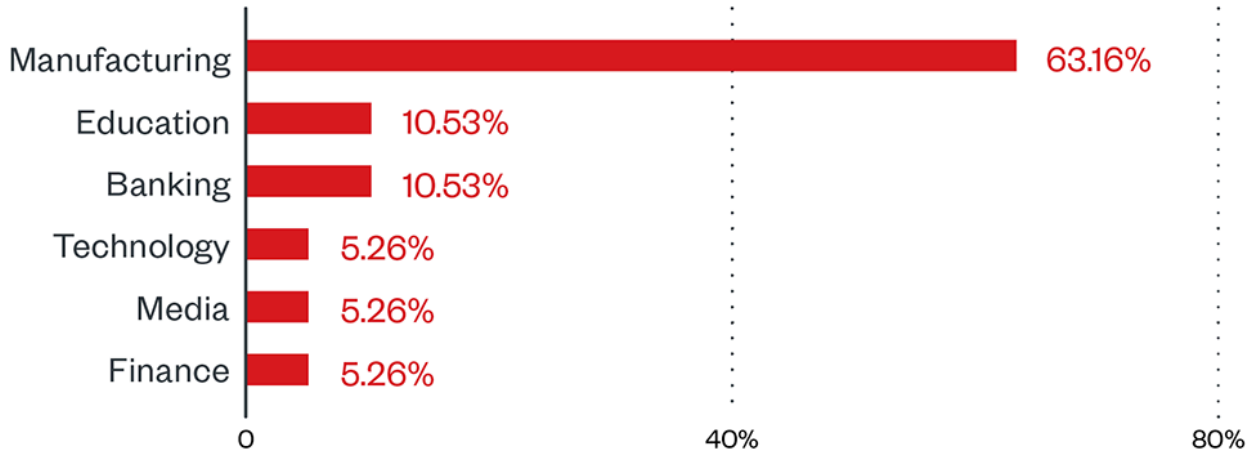
Our telemetry shows data on RansomEXX activity or attack attempts from March 31, 2021 to March 31, 2022. We observed RansomEXX activity from all over the globe, but the heaviest concentration was in USA in France followed by Brazil. The reason behind this observation is the 2021 RansomEXX attack on a major hardware manufacturer in Taiwan.



open on a new tab

Figure 1. Countries with the highest number of attack attempts for the RansomEXX ransomware (March 31, 2021 to March 31, 2022) Source: *Trend Micro™ Smart Protection Network™* ™

Based on our detections, RansomEXX was most active in the manufacturing sector, followed by the education and banking sectors. Overall, the differences are relatively slim given the small sample size.

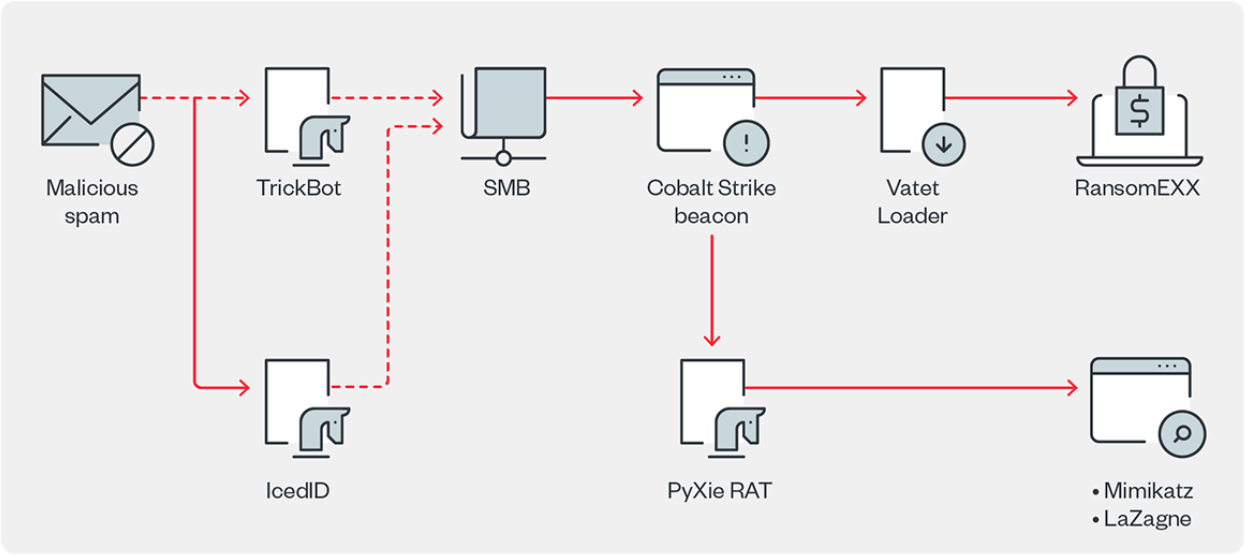


open on a new tab

Figure 2. Industries with the highest number of attack attempts for AvosLocker ransomware (March 31, 2021 to March 31, 2022)Source: *Trend Micro™ Smart Protection Network™*

Infection chain and techniques

Given that RansomEXX operates on the RaaS model, its infection chain can vary depending on the target and the affiliate carrying out the various stages of the attack.



open on a new tab

Figure 3. RansomEXX infection chain

Initial Access

- RansomEXX has been known to use Malspam to infiltrate machines and deliver multiple tools and related malware before finally deploying the actual ransomware payload.

Execution and Exfiltration

- The threat actors make use of different pieces of malware for execution. From our telemetry, we saw IcedID, TrickBot, Cobalt Strike beacons, and PyXie RAT. These are known to be used in other campaigns as well. PyXie RAT also has the capability to exfiltrate data and obtain information from the target machine.

Lateral Movement

- For lateral movement, multiple server message block (SMB) hits were seen on our telemetry. This has been used to deliver VATET loader.

Discovery

- Similar to other campaigns, RansomEXX also makes use of Mimikatz and LaZagne to extract credentials from the target machine.

Impact

- The deployment of the final ransomware payload ensures that files are encrypted in the machine.
- RansomEXX encrypts files using advanced encryption standard (AES), while the AES key is encrypted using RSA encryption.

Other technical details

- It avoids encrypting the following strings in their file path:
    - \windows\system32\
    - \windows\syswow64\
    - \windows\system\
    - \windows\winsxs\
    - \appdata\roaming\
    - \appdata\local\
    - \appdata\locallow\
    - \all users\microsoft\
    - \inetpub\logs\
    - :\boot\
    - :\perflogs\
    - :\programdata\
    - :\drivers\
    - :\wsus\
    - :\efstmpwp\
    - :\$recycle.bin\
    - crypt_detect
    - cryptolocker

    - ransomware
    - ProgramW6432
    - %ProgramFiles%
- It avoids encrypting the following files with strings in their file name:
    - bootsect.bak
    - iconcache.db
    - thumbs.db
    - debug.txt
    - boot.ini
    - desktop.ini
    - autorun.inf
    - ntuser.dat
    - ntldr
    - ntdetect.com
    - bootfont.bin
    - !{Targeted Company Acronym}_READ_ME!.txt
    - ransom
    - ransomware
- It avoids encrypting files with the following extensions:
    - .ani
    - .cab
    - .cpl
    - .diagcab
    - .diagpkg
    - .dll
    - .drv
    - .hlp
    - .icl
    - .icns
    - .ico
    - .iso
    - .ics
    - .lnk
    - .idx
    - .mod
    - .mpa
    - .msc
    - .msp
    - .msstyles
    - .msu
    - .nomedia
    - .ocx

    - .prf
    - .rtp
    - .scr
    - .shs
    - .spl
    - .sys
    - .theme
    - .thempack
    - .exe
    - .bat
    - .cmd
    - .url
    - .mui
    - .{Targeted Company Acronym
- It terminates the following processes:
    - javaw
    - java
    - sage
    - ks_action
    - ks_email
    - ks_copy
    - ks_sched
    - ks_web
    - ks_im
    - ks_db
    - pvxiosvr
    - pvxwin32
    - xfssvccon
    - wordpad
    - wlmail
    - onenote
    - om8start
    - om8
    - ocssd
    - ocomm
    - ocautoupds
    - notepad
    - notepad++
    - node
    - nginx
    - ncsvc
    - ncs

- mydesktopservice
- mydesktopqos
- mspub
- msaccess
- mongod
- metiix
- mdccom
- mbarw
- mail
- i_view32
- infopath
- exchange
- excel
- encsvc
- duplicati
- devenv
- dbsnmp
- dbeng50
- database
- backup
- atom
- arw
- agntsvcencsvc
- agntsvcagntsvc
- agntsvc
- ARSM
- AcrSch2Svc
- Acronis VSS Provider
- AcronisAgent
- AcronixAgent
- Antivirus
- MSSQL$TPS
- MSSQL$TPSAMA
- MSSQL$VEEAMSQL2008R2
- MSSQL$VEEAMSQL2012
- MSSQLFDLauncher
- MSSQLFDLauncher$PROFXENGAGEMENT
- MSSQLFDLauncher$SBSMONITORING
- MSSQLFDLauncher$SHAREPOINT
- MSSQLFDLauncher$SQL_2008
- MSSQLFDLauncher$SYSTEM_BGC
- MSSQLFDLauncher$TPS

- MSSQLFDLauncher$TPSAMA
- MSSQLSERVER
- MSSQLServerADHelper
- MSSQLServerADHelper100
- MSSQLServerOLAPService
- McAfeeEngineService
- McAfeeFramework
- McAfeeFrameworkMcAfeeFramework
- McShield
- McTaskManager
- MongoDB
- MsDtsServer
- MsDtsServer100
- MsDtsServer110
- MySQL57
- MySQL80
- NetMsmqActivator
- OracleClientCache80
- OracleServiceXE
- TrueKey
- TrueKeyScheduler
- TrueKeyServiceHelper
- UI0Detect
- Veeam Backup Catalog Data Service
- VeeamBackupSvc
- VeeamBrokerSvc
- VeeamCatalogSvc
- VeeamCloudSvc
- VeeamDeploySvc
- VeeamDeploymentService
- VeeamEnterpriseManagerSvc
- winword
- vmwp
- vmware-vmx
- vmms
- vmconnect
- vmcompute
- visio
- veeam
- tv_x64
- tv_w32
- tomcat

- thunderbird
- thebat64
- thebat64
- teamviewer
- tbirdconfig
- tasklist
- BackupExecAgentAccelerator
- BackupExecAgentBrowser
- BackupExecDeviceMediaService
- BackupExecJobEngine
- BackupExecManagementService
- BackupExecRPCService
- BackupExecVSSProvider
- DCAgent
- DbxSvc
- EPSecurityService
- EPUpdateService
- ESHASRV
- EhttpSrv
- Enterprise Client Service
- EraserSvc11710
- EsgShKernel
- FA_Scheduler
- IISAdmin
- IMAP4Svc
- KAVFS
- KAVFSGT
- MBAMService
- MBEndpointAgent
- MSExchangeAB
- MSExchangeADTopology
- MSExchangeAntispamUpdate
- MSExchangeES
- MSExchangeEdgeSync
- MSExchangeFBA
- MSExchangeFDS
- MSExchangeIS
- MSExchangeMGMT
- OracleXETNSListener
- PDVFSService
- POP3Svc
- RESvc

- ReportServer
- ReportServer$SQL_2008
- ReportServer$SYSTEM_BGC
- ReportServer$TPS
- ReportServer$TPSAMA
- SAVAdminService
- SAVService
- SDRSVC
- SMTPSvc
- SNAC
- SQL Backups
- SQLAgent$BKUPEXEC
- SQLAgent$CITRIX_METAFRAME
- SQLAgent$CXDB
- SQLAgent$ECWDB2
- SQLAgent$PRACTTICEBGC
- SQLAgent$PRACTTICEMG
- SQLAgent$PROD
- SQLAgent$PROFXENGAGEMENT
- SQLAgent$SBSMONITORING
- SQLAgent$SHAREPOINT
- SQLAgent$SOPHOS
- SQLAgent$SQLEXPRESS
- SQLAgent$SQL_2008
- SQLAgent$SYSTEM_BGC
- SQLAgent$TPS
- SQLAgent$TPSAMA
- VeeamHvIntegrationSvc
- VeeamMountSvc
- VeeamNFSSvc
- VeeamRESTSvc
- VeeamTransportSvc
- W3Svc
- WRSVC
- Zoolz 2 Service
- bedbg
- ekrn
- kavfsslp
- klnagent
- macmnsvc
- masvc
- mfefire

- taskmgr
- synctime
- sublime_text
- stream
- steam
- sqbcoreservice
- screenconnect
- ruby
- qbw32
- pythonw
- python
- processhacker
- powerpnt
- postgres
- php
- outlook
- oracle
- MSExchangeMTA
- MSExchangeMailSubmission
- MSExchangeMailboxAssistants
- MSExchangeMailboxReplication
- MSExchangeProtectedServiceHost
- MSExchangeRPC
- MSExchangeRepl
- MSExchangeSA
- MSExchangeSRS
- MSExchangeSearch
- MSExchangeServiceHost
- MSExchangeThrottling
- MSExchangeTransport
- MSExchangeTransportLogSearch
- MSOLAP$SQL_2008
- MSOLAP$SYSTEM_BGC
- MSOLAP$TPS
- MSOLAP$TPSAMA
- MSSQL$BKUPEXEC
- MSSQL$ECWDB2
- MSSQL$PRACTICEMGT
- MSSQL$PRACTTICEBGC
- MSSQL$PROD
- MSSQL$PROFXENGAGEMENT
- MSSQL$SBSMONITORING

- MSSQL$SHAREPOINT
- MSSQL$SOPHOS
- MSSQL$SQLEXPRESS
- MSSQL$SQL_2008
- MSSQL$SYSTEM_BGC
- SQLAgent$VEEAMSQL2008R2
- SQLAgent$VEEAMSQL2012
- SQLBrowser
- SQLSERVERAGENT
- SQLSafeOLRService
- SQLTELEMETRY
- SQLTELEMETRY$ECWDB2
- SQLWriter
- SQLsafe Backup Service
- SQLsafe Filter Service
- SamSs
- SepMasterService
- ShMonitor
- SmcService
- Smcinst
- SntpService
- Sophos Agent
- Sophos AutoUpdate Service
- Sophos Clean Service
- Sophos Device Control Service
- Sophos File Scanner Service
- Sophos Health Service
- Sophos MCS Agent
- Sophos MCS Client
- Sophos Message Router
- Sophos Safestore Service
- Sophos System Protection Service
- Sophos Web Control Service
- SstpSvc
- Symantec System Recovery
- TmCCSF
- mfemms
- mfevtp
- mozyprobackup
- msftesql$PROD
- ntrtscan
- sacsvr

- sophossps
- svcGenericHost
- swi_filter
- swi_service
- swi_update
- swi_update_64
- tmlisten
- wbengine

MITRE tactics and techniques

Initial Access	Execution	Defense Evasion	Discovery	Impact
T1078 - Valid Accounts *Like other human-operated ransomware families, it can arrive by brute-forcing weak remote desktop protocol (RDP) credentials*	**T1059.003** - Command-Line Interface: Windows Command Shell *Can be executed using cmd.exe*	**T1140** - Deobfuscate/Decode Files or Information *Some strings used, such as the strings that will be displayed on the console, are encrypted, and will only be decrypted when needed* **T1562.001** - Impair Defenses: Disable or Modify Tools *RansomEXX stops services related to security software to avoid being detected*	**T1082** - System Information Discovery *It gathers the system's computer name, which it uses to create a mutex* **T1049** - System Network Connections Discovery *It enumerates available network resources on the infected machine to look for files to*	**T1489** - Service stop *The ransomware stops services to avoid file access violations when encrypting files that are still being accessed* **T1490** -Inhibit system recovery *Inhibits restoration of files from backup by executing the following commands:* *- wbadmin.exe delete catalog -quiet* *- bcdedit.exe /set {default} recoveryenabled no* *- bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures* *- schtasks.exe /Change /TN "\Microsoft\Windows\SystemRestore\SR" /disable fsutil.exe usn deletejournal /D C:*

Initial Access	Execution	Defense Evasion	Discovery	Impact
			encrypt; it does this by using the Wnet API's **T1083 -** File and Directory Discovery *For its file encryption, it enumerates files and directories on each drive while avoiding safe-listed files or directories* **T1486 -** Data encrypted for impact *It encrypts files using AES encryption while the AES key is encrypted using RSA encryption*	

Summary of malware, tools, and exploits used

Security teams can watch out for the presence of the following malware tools and exploits that are typically used in RansomEXX attacks:

Initial Access	Execution	Discovery	Lateral Movement	Impact
• Malspam	• IcedID	• Mimikatz	• SMB	• RansomEXX
	• TrickBot	• LaZagne		
	• PyXie RAT			
	• Cobalt Strike beacon			
	• Vatet Loader			

Recommendations

RansomEXX is not as active as it had been in 2020, when its consecutive attacks made it one of the newer ransomware families to watch out for. However, being a highly targeted and human-operated ransomware, its attacks affect its victims and their reputation significantly. The combination of memory-based techniques, legitimate Windows tools, and post-intrusion contribute a lot to RansomEXX's successes.

Preventing the attacks from the outset is key to avoiding the worst of ransomware campaigns. Organizations should learn from past RansomEXX campaigns and be vigilant against initial access tactics. Users should be wary of enabling macros, and of documents that prompt them to do so.

To help defend systems against similar threats, organizations can establish security frameworks that can allocate resources systematically for establishing solid defenses against ransomware.

Here are some best practices that can be included in these frameworks:

Audit and inventory

- Take an inventory of assets and data.
- Identify authorized and unauthorized devices and software.
- Make an audit of event and incident logs.

Configure and monitor

- Manage hardware and software configurations.
- Grant admin privileges and access only when necessary to an employee's role.

- Monitor network ports, protocols, and services.
- Activate security configurations on network infrastructure devices such as firewalls and routers.
- Establish a software allowlist that only executes legitimate applications.

Patch and update

- Conduct regular vulnerability assessments.
- Perform patching or virtual patching for operating systems and applications.
- Update software and applications to their latest versions.

Protect and recover

- Implement data protection, back up, and recovery measures.
- Enable multifactor authentication (MFA).

Secure and defend

- Employ sandbox analysis to block malicious emails.
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network.
- Detect early signs of an attack such as the presence of suspicious tools in the system.
- Use advanced detection technologies such as those powered by AI and machine learning.

Train and test

- Regularly train and assess employees on security skills.
- Conduct red-team exercises and penetration tests.

A multilayered approach can help organizations guard possible entry points into the system (endpoint, email, web, and network). Security solutions that can detect malicious components and suspicious behavior can also help protect enterprises.

- Trend Micro Vision One™products provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before the ransomware can do irreversible damage to the system.
- Trend Micro Cloud One™products Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™products Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™products offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---