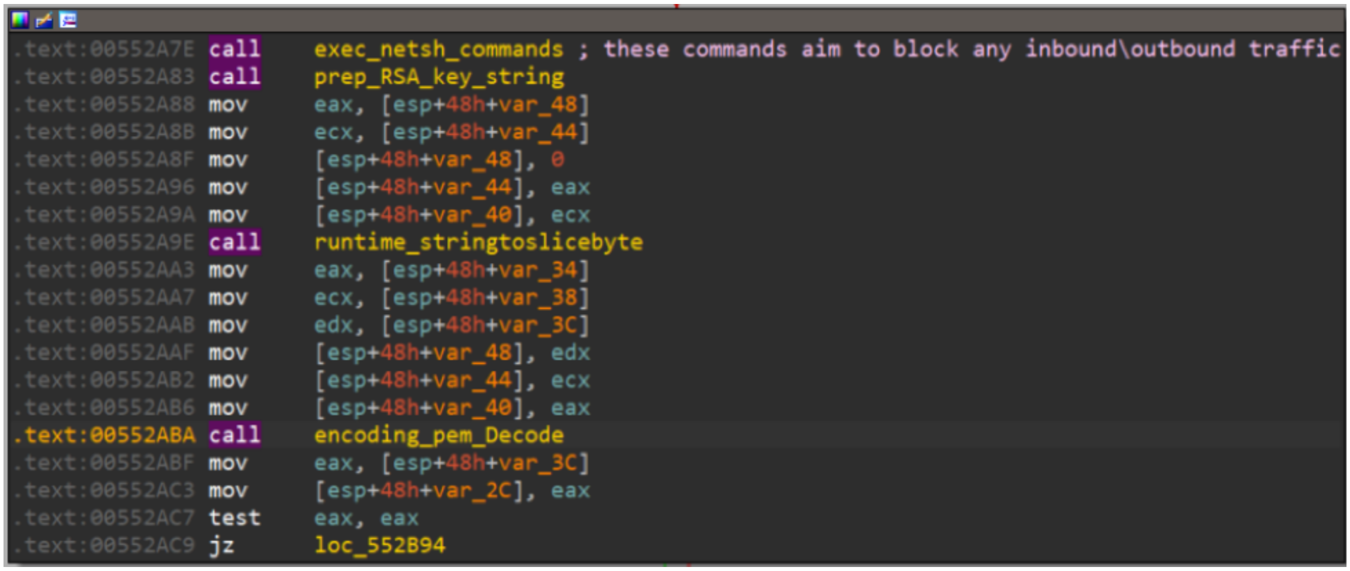
EKANS Ransomware: A Malware Targeting OT ICS Systems

fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems

July 1, 2020



```
.text:00552A7E call    exec_netsh_commands ; these commands aim to block any inbound\outbound traffic
.text:00552A83 call    prep_RSA_key_string
.text:00552A88 mov     eax, [esp+48h+var_48]
.text:00552A8B mov     ecx, [esp+48h+var_44]
.text:00552A8F mov     [esp+48h+var_48], 0
.text:00552A96 mov     [esp+48h+var_44], eax
.text:00552A9A mov     [esp+48h+var_40], ecx
.text:00552A9E call    runtime_stringtoslicebyte
.text:00552AA3 mov     eax, [esp+48h+var_34]
.text:00552AA7 mov     ecx, [esp+48h+var_38]
.text:00552AAB mov     edx, [esp+48h+var_3C]
.text:00552AAF mov     [esp+48h+var_48], edx
.text:00552AB2 mov     [esp+48h+var_44], ecx
.text:00552AB6 mov     [esp+48h+var_40], eax
.text:00552ABA call    encoding_pem_Decode
.text:00552ABF mov     eax, [esp+48h+var_3C]
.text:00552AC3 mov     [esp+48h+var_2C], eax
.text:00552AC7 test    eax, eax
.text:00552AC9 jz      loc_552B94
```

Threat Research

By Ben Hunter and Fred Gutierrez | July 01, 2020

According to the 2020 Verizon Data Breach Investigations Report, ransomware accounted for 27% of malware incidents in 2019. This may not seem like a lot, but when you think of the impact it has on an organization you can understand why it’s often the malware that makes the news headlines. Over the last few years, the impact has worsened due to adversaries moving to a more targeted attack method, rather than the traditional “spray and pray” method of infecting as many potential victims as possible.

This up-front investment in time and resources has shown to be fruitful for attackers, especially as they focus on specific industries, with healthcare as well as states and local governments emerging as high-profile targets during the course of 2020. The latest industry targeted with ransomware is Industrial Control Systems/Operational Technology. This blog will break down at a high level the latest EKANS ransomware, general TTP trends, and related protections for targeted ransomware attacks.

Affected platforms: Windows Operating Systems
Impacted parties: Industrial Control Systems and a variety of applications
Impact: Data Encryption for Impact – Mitre ID:T1486
Severity level: High

EKANS Ransomware

Through one of our trusted partnerships, FortiGuard Labs was provided with an EKANS sample to analyze around the end of May. A more recent June version was independently sourced by FortiGuard Labs.

MD5	SHA256
May Variant	
47EBE9F8F5F73F07D456EC12BB49C75D	2ED3E37608E65BE8B6E8C59F8C93240BD0EFE9A60C08C21F4889C00EB6082D74
June Variant	
ED3C05BDE9F0EA0F1321355B03AC42D0	D4DA69E424241C291C173C8B3756639C654432706E7DEF5025A649730868C4A1

Each of these samples are written in the GO programming language. The GO programming language first appeared around 2009 and has slowly gained popularity within the malware community.

The Difficulty of Analyzing EKANS Malware - “Go”ing to Create a Custom IDA Plugin

One of the advantages of GO is that the code can be easily compiled to work on different platforms and architectures, such as MacOS, Microsoft Windows, and the Linux operating system when compared to other programming languages. One of the disadvantages, however, is that the binaries are noticeably larger in size. A simple “Hello World” program can produce a binary 1 MB in size. To combat bulky file sizes, GO allows a programmer to strip binaries during compilation. Most of the information that gets removed is typically used by debuggers.

As it turns out, this size problem is actually helpful to malware authors. By having a larger file size, manual analysis will inevitably take longer. Moreover, it can easily be overlooked since typical malware files have a much smaller file size in the first place. By stripping the binaries of debugging information, malware analysts will have another stumbling block to overcome.

Looking at the given files closer, we can see that they are indeed stripped and offer no clues for the malware analyst.

Figure 1. Number of Functions to Analyze

The typical malware may have hundreds of functions, and some will already be recognized in the malware analysis industry’s unofficial default disassembler, IDA. With stripped GO binaries, however, IDA is unable to recognize normal library files, leaving the malware analyst with more than 5000 functions to sift through.

Because of this problem, we developed an EKANS-specific IDA plugin in-house to help with analysis in conjunction with other GO-specific analysis techniques.

Figure 2. Custom IDA Plugin Developed by FortiGuard Labs

As can be seen above, there are over 2100 encrypted strings, almost 2400 obfuscated function names, and over 1200 strings that needed fixing in the May variant of EKANS.

Both of these variants perform all of the typical ransomware activities you would expect, such as encrypting files and leaving a ransom note telling the victim to contact them at a specified email address, to receive instructions on how to pay a ransom and decrypt their files. But they also perform actions that are not so typical. Below is a high-level list of these activities in sequence, with the main notable difference of turning off the host firewall, found in the June variant:

- Confirms Target Environment
- Isolates the Infected System (Host Firewall)
- The public RSA Key used in the file encryption process is decoded
- Identifies and Stops Specific Services and Processes
- Deletes Shadow Copy
- Encrypts Files
- Turns Off Host Firewall

Figure 3. High-Level Flow of EKANS ransomware functions

It is important to note that turning off the host firewall seems to have been a new addition to the malware family’s functionality. This was not present in the older May variant. Another interesting addition was to turn on the firewall before encrypting, probably to detect AVs and other defense solutions by blocking any communication from the agent.

Confirming the Target Environment for EKANS Ransomware

The ransomware starts out by attempting to confirm its target by resolving the domain belonging to the victim’s company, as well as comparing the resolved domain to a specific IP. If the domain/IP is not available, the routine exits.

Figure 4. Malware confirming its target

Looking deeper into the environmental checks, we noticed that the May variant of EKANS tries to resolve the IP address of the ADS.****.COM. The subdomain belongs to a global health care provider that specializes in the treatment of chronic kidney conditions.

Figure 5. Subdomain IP Check

This subdomain does not seem to be publicly available, which means that the May variant will only execute if it has infiltrated the network. If this is successful, then another check is performed. EKANS checks to see if *“10.2.10.4”* is the IP address of this subdomain.

Figure 6. IP Compare

Another piece of information that the May variant of EKANS is looking for is the current machine’s role within the domain.

Figure 7. Domain Role Check

A WMI query will be performed to determine this. Microsoft defines domain roles as the following.

0	Standalone Workstation
1	Member Workstation
2	Standalone Server
3	Member Server
4	Backup Domain Controller
5	Primary Domain Controller

EKANS is apparently looking to infect a domain controller on the network. If successful, this can affect security authentication requests within the network domain, thereby severely impacting networked users. With the aforementioned data points, EKANS will have enough to build a proper mutex.

Figure 8. Mutex Creation

The mutex will consist of the string *“Global\”* appended with *“EKANS”* and a part of the IP string. On a side note, the author(s) of EKANS may be a fan of The Highlander movies/TV series where the phrase “*there can be only one*” was popularized.

Figure 9. Exit Message

Isolating a System Infected by EKANS Ransomware

The next step taken by the June variant of the ransomware that FortiGuard Labs engineers encountered was that the malware executed the following netsh commands in order to block any inbound and outbound traffic that might interfere with the encryption process:

- *netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound*
- *netsh advfirewall set allprofiles state on*

Figure 10. Malware isolating infected system

Figure 11. netsh.exe running to change host firewall settings.

Decoding EKANS Ransomware’s Public RSA Key

Next, the malware goes through its encryption functions, which like many ransomware variants are embedded in the malware. It encrypts data using RSA and by parsing the public key using the ParsePKCS1PublicKey function. It is XOR decoded.

Figure 12. RSA key decoded

Figure 13. Public key being parsed by the ParsePKCS1PublicKey function

EKANS Malware Identifies and Stops Services and Processes

In both variants, EKANS will decode strings associated with services and attempt to stop them. The May variant, for some reason, contains duplicate services.

Figure 14. Service Redundancy

Overall, there are nine services that are repeatedly decrypted in an attempt to stop them by the May variant of EKANS. They are:

MSSQLFDLauncher$PROFXENGAGEMENT, ReportServer$TPS, SQLBrowser, MSSQLServerADHelper, SQLAgent$PROD, msftesql$PROD, SQLAgent$SOPHOS, VeeamEnterpriseManagerSvc, and ArcserveUDPPS

After decoding all the required strings (see Appendix A), both variants of the ransomware open the SCM (OpenSCManager) and use EnumServicesStatusEx. It iterates on the services and stops any service contained in the decoded string list.

The service stop operation stops:

- OpenService (SC_MANAGER_ENUMERATE_SERVICE)
- ServiceControl (SERVICE_CONTROL_STOP)
- ServiceQuery

Figure 15. Identifies and stops specific services.

EKANS Also Identifies and Kills Processes

The ransomware then enumerates running processes and terminates each process within a predefined process list (See Appendix-B). The following code handles the process termination:

Figure 16. Malware terminates specific processes.

EKANS Deletes Shadow Copies

EKANS then deletes shadow copies, which is done via WMI's WbemScripting.SWbemNamedValueSet object. The query that locates the shadow copies object is the regular:

```
SELECT * FROM Win32_ShadowCopy
```

This is common behavior with ransomware to make it more difficult to recover files. There are many ways to achieve this. If you're interested in learning more, please read Ben Hunter's "Stomping Shadow Copies – A second Look into Deletion Methods" blog.

The May variant accomplishes this by using COM programming. EKANS connects to the WMI service via COM objects in order to use shared libraries utilizing code similar to https://raw.githubusercontent.com/go-ole/go-ole/master/guid.go, which is used by various other legitimate GO software, as well as other malicious binaries.

Figure 17. COM Objects Used

EKANS Ransomware Encrypts Files

Before running the encryption function, the ransomware decodes the strings of all of the relevant file extensions to encrypt, (see Appendix-C).

In order to keep the system able to at least spin up and load, certain files and folders are skipped from the encrypting process. These files are avoided in the May variant of EKANS.

Figure18. Files Avoided by the May Variant

At the same time, any files and folders that contain the following directories in their path are also skipped from the file encryption process by the May variant.

Figure 19. Folders Avoided by May Variant

The following file types are also avoided by the May variant.

Figure 20. File types Avoided by May Variant

Both variants also build the following regex used to exclude encryption targets.

Figure 21. Malware excluding encryption targets

However, during the actual file encryption process, the list of targeted file types is not actually checked by the May variant of the ransomware. The May variant will encrypt any file type as long as it does not violate any of its avoidance rules.

The encryption details seem identical to the operating methods described here: https://www.ccn-cert.cni.es/pdf/5045-ccn-cert-id-15-20-snake-locker-english-1/file.html

- A public RSA key is used to encrypt each of the AES keys used to encrypt files.
- File encryption is via AES CTR mode, with a random key and a random IV.
- The AES key is ciphered with RSA-OAEP, and uses *ripemd160* as its hashing algorithm.
- The AES encrypted key, along with the original file name, is encoded using GOB (an algorithm from Golang), and it is written at the end of the file.

First, it enumerates all valid drive letters from A to Z using GetLogicalDriveStringsW.

Figure 22. Drive Enumeration

Interestingly enough, the code shown in the figure below shows that the May variant of EKANS only targets removable drives (such as thumb drives) and fixed drives (such as hard disks or flash storage devices). They do not try to infect machines on the network.

Figure 23. Drive Types Targeted

It then creates multiple threads for such drives.

Figure 24. Enumerating valid drive letters.

Each thread then creates eight workers (threads) that perform the encryption. These workers use channels to sync themselves.

Figure 25. Threads performing encryption

After creating the eight workers, the thread waits for them to finish. After all of them are done, it renames the files on the system by generating a random 5-digits string which is then appended to the file’s name.

Figure 26. Malware renaming files.

The single file encryption flow is relatively simple:

- Opens a file
- Checks to see if it already has the *EKANS* stamp at the file’s end. If not, it encrypts the file via AES as seen in the following loop:
- Encryption (it overwrites the file, not creating a new one)

First, initiates a cipher:

Figure 27. Malware initiates Cipher

After the encryption process has completed, the May variant of EKANS drops the ransom note as *“Decrypt-Your-Files.txt”* either on the root system drive or on the user’s desktop.

Figure 28. Ransom Note

Finally, EKANS Turns Off Host Firewall

For machines infected with the June variant, the ransomware ends with another command to turn off the firewall.

EKANS Mitre TTPs

Execution

Component Object Model and Distributed COM (Mitre ATT&CK ID: T1175)
EKANS executes WMI queries via COM objects

Defense Evasion

- Disabling Security Tools (Mitre ATT&CK ID: T1089)
  EKANS attempts to disable processes and kill services (see Appendix)
- Execution Guardrails (Mitre ATT&CK ID: T1480)
  EKANS will check network, IP, and domain role

- Indirect Command Execution (Mitre ATT&CK ID: T1202)
  - netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound
  - netsh advfirewall set allprofiles state on
- Virtualization/Sandbox Evasion (Mitre ATT&CK ID: T1497)
  EKANS attempts to disable virtualization services and processes (see Appendix)

Discover

File and Directory Discovery (Mitre ATT&CK ID: T1083)
EKANS builds a list of files and directories that need to be encrypted

Peripheral Device Discovery (Mitre ATT&CK ID: T1120)
EKANS will attempt to encrypt files on removable drives such as USB drives

Process Discovery (Mitre ATT&CK ID: T1057)
EKANS will attempt to terminate certain processes (see Appendix)

Security Software Discovery (Mitre ATT&CK ID: T1063)
EKANS will attempt to disable certain security software (see Appendix)

Software Discovery (Mitre ATT&CK ID: T1518)
EKANS will attempt to disable certain ICS processes (see Appendix)

System Information Discovery (Mitre ATT&CK ID: T1082)

- EKANS checks for the existence of a mutex
- EKANS checks for the system’s role in the domain

System Network Configuration Discovery (Mitre ATT&CK ID: T1049)
EKANS queries the network to see if it is part of the targeted domain

System Service Discovery (Mitre ATT&CK ID: T1007)
EKANS will attempt to halt certain services (see Appendix)

Virtualization/Sandbox Evasion (Mitre ATT&CK ID: T1497)
EKANS attempts to disable virtualization services and processes (see Appendix)

Impact

Data Encrypted for Impact (Mitre ATT&CK ID: T1486)
EKANS will encrypt certain files to be ransomed

Inhibit System Recovery (Mitre ATT&CK ID: T1490)
EKANS deletes shadow copies to prevent recovery of encrypted files

Network Denial of Service (Mitre ATT&CK ID: T1498)
Infected domain controllers may prevent users from logging into the network

Service Stop (Mitre ATT&CK ID: T1489)
EKANS will attempt to halt certain services (see Appendix)

General TTP Trends

Understanding the ransomware and some of its indicators of compromise (IOC), such as hashes, URLs, IP addresses, and domains is a good first defense. But be warned that these IOCs often change and can circumvent legacy security controls. And because these attacks are more targeted, it’s also important to understand the activity the offensive operator takes once they’re in the environment. If you can disrupt their plans prior to the malware executing, the better off you will be. While every targeted attack is unique, there are some trends – especially in the way an attacker works – that if understood can provide a better view into your ability to detect their attack methods and more effectively block them.

Let’s take a look into some of the trends we often see from our FortiGuard Managed Detection and Response and Incident Response Services.

Initial Access

There are many ways to access a network, but the two we continue to observe are:

- External Remote Services (Mitre ATT&CK ID:T1133)
  Exploiting existing vulnerabilities and weak credentials on RDP sessions that are publicly exposed.
- Spear phishing Attachments and Links (Mitre ATT&CK ID:T1193 and ID:T1192)
  The malware delivery of choice these days is still by sending a spear phishing email.

OS Credential Dumping

Once the adversary establishes their initial access into the environment, they need to continue penetrating deeper into the network. To do so, they first need the right access, which is why credential dumping is a common activity. There are many techniques to achieve the dumping of credentials, as the Windows Operating System has many different places it stores or caches its credentials. Below is one common technique we see as a trend:

OS Credential Dumping – LSASS Memory (Mitre ATT&CK ID:T1003.001)
The LSASS process stores credentials of users that are logged in to a system. Many tools are available to extract this credential information.

If you want to read more on OS Credential Dumping, please view our Offense and Defense – A Tale of Two Sides: (Windows) OS Credential Dumping blog.

Lateral Movement

When the adversary has the right access to spread their malware from system to system, they simply need to copy and remotely execute the payload. One tool that can achieve just that is found on many Windows Operating Systems. It is called PSEXEC, which is part of the Sysinternals. This tool is used by many system admins to help administer the network, but it is also often used by the adversary.

Lateral Tool Transfer (Mitre ID:T1570)
Many tools can be used to copy and remotely execute a piece of software. The PSEXEC tool is one of them. When psexec.exe runs, it will copy the psexecsvc.exe file to the remote system, which is used to start and run the malicious software as a service. It’s also worth mentioning that it will use Windows admin shares such as C$, IPS$, ADMIN$.

Defensive Evasion

As a security community we have gotten better at identifying malicious software and tools. As a result, adversaries have had to take that into consideration by adding additional steps to disable defensive controls such as anti-malware, or by disabling Windows event logging.

- Impair Defenses - Disable or Modify Tools (Mitre ID:T1562.001)
  If the adversary has administrator access it may be possible to uninstall or shutdown services such as Microsoft Defender. They will uninstall the service, run their malware, and then reinstall the services.
- Impair Defenses - Disable Windows Event Logging (Mitre ID:T1562.002)
  Logs are a great source for detecting anomalies on your hosts, and companies are collecting these logs centrally and monitoring them for those anomalies. To address this process, adversaries will disable event logging or suppress logs so they can’t be viewed by the monitoring tool or process.

Defensive Evasion/Privilege Escalation/Persistence

Eventually, the attacker will execute the ransomware (or malware in general) on targeted systems. An efficient way to do this, if the attacker has access to the domain controllers, is to leverage group policies (GPO) and Windows login scripts. GPOs and login scripts are used by system admins for central management and OS configuration setting for users’ environments. These tools, which are part of an Active Directory environment, are modified by an attacker to deploy and execute their malware.

- Group Policy Modification (GPO) (Mitre ID:T1484)
  The attacker can create a group policy preference scheduled task policy within a Default Domain Policy that will deliver the malware and execute it on all machines within the AD domain.
- Boot or Logon Initialization Scripts: Login Script – Windows (Mitre ID:T1037.001)
  Because logon scripts can be run when users login to systems in an AD domain, an attacker can add their malicious payload to the script to execute.

Conclusion: Prepare for Ransomware Threats Beyond EKANS

In this blog we focused on not only one of the latest ransomware variants targeting ICS/OT environments, but also some of the TTP trends our FortiGuard team has observed over the last year or two. We encourage you to take a look at not only the techniques we described here, but also at the other techniques that are documented in the Mitre ATT&CK knowledge base. Then start testing your current security controls against these techniques to ensure you can detect or protect against them.

If you find gaps, document them and use them as a guide to build a prioritized action plan for improvement. Lastly, if you are responsible for the ICS environment there is now a Mitre ATT&CK ICS knowledge base specifically for adversary actions taking place in an Industrial Control System network.

How Fortinet Protects Organizations from EKANS

Fortinet offers a suite of platforms and services to help protect organizations from ransomware and malware, including EKANS. Here's how it works:

FortiEDR Platform: Identification & Blocking of EKANS

Fortinet's FortiEDR Platform detects and blocks the EKANS malware. When activity tries to run, such as changing the Windows firewall settings or encrypting files, FortiEDR identifies and blocks the malicious activity.

Figure 29. FortiEDR blocking malicious netsh.exe activity.

Figure 30. FortiEDR identifying specific command line activity.

Figure 31. FortiEDR blocking the file encryption activity.

FortiGuard Anti-Virus Services

These ransomware variants are blocked with the signatures W32/Ekans.42D0!tr.ransom, W32/Ekans.C75D!tr.ransom, and W32/Ekans.62B8!tr.ransom.

FortiDeceptor: Deception-based Breach Protection

FortiDeceptor allows organizations to rapidly create a fabricated deception network through the automatic deployment of decoys and lures that seamlessly integrate with an existing IT/OT infrastructure, enticing attackers into revealing themselves. FortiDeceptor helps serve as an early warning system by providing accurate detection that correlates an attacker's activity details and lateral movement that feeds up to a broader threat campaign. Threat intelligence captured from decoys is shared within the Security Fabric so automatic protection can be applied, disrupting attacks before any real damage is done.

Appendix A – Services Targeted by EKANS

May Variant

Acronis VSS Provider, Enterprise Client Service, 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, SQLsafe Backup Service, SQLsafe Filter Service, Symantec System Recovery, Veeam Backup Catalog Data Service, AcronisAgent, AcrSch2Svc, Antivirus, ARSM, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDeviceMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, BackupExecVSSProvider, bedbg, DCAgent, EPSecurityService, EPUpdateService, EraserSvc11710, EsgShKernel, FA_Scheduler, IISAdmin, IMAP4Svc, macmnsvc, masvc, MBAMService, MBEndpointAgent, McAfeeEngineService, McAfeeFramework, McAfeeFrameworkMcAfeeFramework, McShield, McTaskManager, mfemms, mfevtp, mozyprobackup, MsDtsServer, MsDtsServer100, MsDtsServer110, MSExchangeES, MSExchangeIS, MSExchangeMGMT, MSExchangeMTA, MSExchangeSA, MSExchangeSRS, MSOLAP$SQL_2008, MSOLAP$SYSTEM_BGC, MSOLAP$TPS, MSOLAP$TPSAMA, MSSQL$BKUPEXEC, MSSQL$ECWDB2, MSSQL$PRACTICEMGT, MSSQL$PRACTTICEBGC, MSSQL$PROFXENGAGEMENT, MSSQL$SBSMONITORING, MSSQL$SHAREPOINT, MSSQL$SQL_2008, MSSQL$SYSTEM_BGC, MSSQL$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, MSSQLServerADHelper100, MSSQLServerOLAPService, MySQL57, ntrtscan, OracleClientCache80, PDVFSService, POP3Svc, ReportServer, ReportServer$SQL_2008, ReportServer$SYSTEM_BGC, ReportServer$TPS, ReportServer$TPSAMA, RESvc, sacsvr, SamSs, SAVAdminService, SAVService, SDRSVC, SepMasterService, ShMonitor, Smcinst, SmcService, SMTPSvc, SNAC, SntpService, sophossps, SQLAgent$BKUPEXEC, SQLAgent$ECWDB2, SQLAgent$PRACTTICEBGC, SQLAgent$PRACTTICEMGT, SQLAgent$PROFXENGAGEMENT, SQLAgent$SBSMONITORING, SQLAgent$SHAREPOINT, SQLAgent$SQL_2008, SQLAgent$SYSTEM_BGC, SQLAgent$TPS, SQLAgent$TPSAMA, SQLAgent$VEEAMSQL2008R2, SQLAgent$VEEAMSQL2012, SQLBrowser, SQLSafeOLRService, SQLSERVERAGENT, SQLTELEMETRY, SQLTELEMETRY$ECWDB2, SQLWriter, SstpSvc, svcGenericHost, swi_filter, swi_service, swi_update_64, TmCCSF, tmlisten, TrueKey, TrueKeyScheduler, TrueKeyServiceHelper, UI0Detect, VeeamBackupSvc, VeeamBrokerSvc, VeeamCatalogSvc, VeeamCloudSvc, VeeamDeploymentService, VeeamDeploySvc, VeeamEnterpriseManagerSvc, VeeamMountSvc, VeeamNFSSvc, VeeamRESTSvc, VeeamTransportSvc, W3Svc, wbengine, WRSVC, VeeamHvIntegrationSvc, swi_update, SQLAgent$CXDB, SQLAgent$CITRIX_METAFRAME, SQL Backups, MSSQL$PROD, Zoolz 2 Service, MSSQLServerADHelper, SQLAgent$PROD, msftesql$PROD, NetMsmqActivator, EhttpSrv, ekrn, ESHASRV, MSSQL$SOPHOS, SQLAgent$SOPHOS, klnagent, MSSQL$SQLEXPRESS, SQLAgent$SQLEXPRESS, kavfsslp, KAVFSGT, KAVFS, mfefire, avast! Antivirus, aswBcc, Avast Business Console Client Antivirus Service, mfewc, Telemetryserver, WdNisSvc, WinDefend, MCAFEETOMCATSRV530, MCAFEEEVENTPARSERSRV, MSSQLFDLauncher$ITRIS, MSSQL$EPOSERVER, MSSQL$ITRIS, SQLAgent$EPOSERVER, SQLAgent$ITRIS, SQLTELEMETRY$ITRIS, MsDtsServer130, SSISTELEMETRY130, MSSQLLaunchpad$ITRIS, BITS, BrokerInfrastructure, epag, EPIntegrationService, EPProtectedService, epredline, TmPfw, SentinelAgent, SentinelHelperService, LogProcessorService, SentinelStaticEngine, DB2GOVERNOR_DB2COPY1, DB2LICD_DB2COPY1, DB2MGMTSVC_DB2COPY1, DB2REMOTECMD_DB2COPY1, DB2DAS00, DB2-0, DB2INST2, IBMDataServerMgr, IBMDSServer41, MSSQL$CITRIX_METAFRAME, RumorServer, myAgtSvc, McAfee SiteAdvisor Enterprise Service, Alerter, ERSvc, Eventlog, ImapiService, NetDDE, NtLmSsp, NtmsSvc, odserv, SnowInventoryClient, TlntSvr, VMTools, VMware, WebClient, WinVNC4, BlueStripeCollector, Cissesrv, CpqRcmc3, gupdate, gupdatem, HealthService, NimbusWatcherService, ProLiantMonitor, SDD_Service, sysdown, System, GoogleChromeElevationService, bcrservice, ccEvtMgr, ccSetMgr, CSAdmin, CSAuth, CSDbSync, CSLog, CSMon, CSRadius, CSTacacs, Symantec, VGAuthService, SepMasterServiceMig, vmware-converter-agent, vmware-converter-server, vmware-converter-worker, avbackup, MSSQL$NET2, Net2ClientSvc, NetSvc, SQLAgent$NET2, tpautoconnsvc, TPVCGateway, VMwareCAFCommAmqpListener, VMwareCAFManagementAgentHost, AdobeARMservice, RSCDsvc, LRSDRVX, msvsmon90, IDriverT, MSMQ, MMS, MSSQLFDLauncher$PROFXENGAGEMENT, ReportServer$TPS, SQLBrowser, MSSQLServerADHelper, SQLAgent$PROD, msftesql$PROD, SQLAgent$SOPHOS, AVP, VeeamEnterpriseManagerSvc, MySQL80, MSSQL$ARCSERVE_APP, ArcserveUDPPS, CAARCAppSvc, CASDatastoreSvc, CASARPSWebSVC, CAARCUpdateSvc, ArcserveUDPPS, CASAD2DwebSvc, ASLogWatch, FireEye Endpoint Agent, nxlog, SplunkForwarder, SAP, MSSQL, MySQL, OracleService, oracleservice, mssql, Sophos, Veeam, Cylance

June Variant

AcrSch2Svc, Antivirus, ARSMbedbgDCAgent, EPUpdateService, EraserSvc11710, EsgShKernel, FA_Scheduler, IISAdminIMAP4Svcmacmnsvcmasvc, MBAMService, MBEndpointAgent, McAfeeFramework, McShieldmfemms, McTaskManager, MsDtsServer, MsDtsServer100, MsDtsServer110, MSExchangeES, MSExchangeIS, MSExchangeMGMT, MSExchangeMTA, MSExchangeSA, MSExchangeSRS, MSSQLFDLauncher, MSSQLSERVER, ntrtscanPOP3Svc, PDVFSService, ReportServer, sacsvr, SamSs, SAVServiceSAVAdminService, SDRSVCShMonitor, SepMasterServiceSmcinstSMTPSvc, SmcService, SNACSntpService, SQLBrowser, SQLSERVERAGENT, SQLTELEMETRY, SQLWriter, svcGenericHost, swi_filterTmCCSFswi_service, swi_update_64, tmlistenTrueKey, TrueKeySchedulerUI0DetectW3Svc, VeeamBackupSvc, VeeamBrokerSvc, VeeamCatalogSvc, VeeamCloudSvc, VeeamDeploySvc, VeeamMountSvc, VeeamNFSSvc, VeeamRESTSvc, wbengineWRSVC, swi_update, NetMsmqActivatorEhttpSrvekrn, ESHASRV, KAVFSmfefire, Telemetryserver, WdNisSvcBITSepagWinDefend, MsDtsServer130, SSISTELEMETRY130epredlineTmPfw, SentinelAgent, DB2INST2myAgtSvcIBMDataServerMgrIBMDSServer41, RumorServer, AlerterERSvc, EventlogNetDDE, ImapiService, NtLmSspNtmsSvc, odservTlntSvr, VMTools, VMware, WebClientWinVNC4CissesrvCpqRcmc3gupdate, gupdatemHealthService, ProLiantMonitor, SDD_Service, sysdown, System, bcrservice, ccEvtMgrccSetMgrCSAdmin, CSAuth, CSDbSyncCSLog, CSMon, CSRadiusCSTacacsSymantecVGAuthService, avbackupNetSvc, Net2ClientSvc, tpautoconnsvc, TPVCGateway, AdobeARMservice, RSCDsvcLRSDRVX, msvsmon90, IDriverTMSMQMMS, MySQL80nxlogSAP, ArcserveUDPPS, CAARCAppSvc, CASDatastoreSvc, CASARPSWebSVC, CAARCUpdateSvc, ArcserveUDPPS, CASAD2DwebSvc, ASLogWatch, SplunkForwarder, MSSQLMySQLmssql, OracleService, oracleservice, SophosVeeam, Cylance, OpenSCManagerW, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDeviceMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, BackupExecVSSProvider, EPSecurityService, McAfeeEngineService, McAfeeFrameworkMcAfeeFramework, MSSQLServerADHelper100, MSSQLServerOLAPService, OracleClientCache80, SQLSafeOLRService, TrueKeyServiceHelper, VeeamDeploymentService, VeeamEnterpriseManagerSvc, VeeamTransportSvc, VeeamHvIntegrationSvc, MSSQLServerADHelper, MCAFEETOMCATSRV530, MCAFEEEVENTPARSERSRV, BrokerInfrastructure, EPIntegrationService, EPProtectedService, SentinelHelperService, LogProcessorService, SentinelStaticEngine, DB2GOVERNOR_DB2COPY1, DB2MGMTSVC_DB2COPY1, DB2REMOTECMD_DB2COPY1, SnowInventoryClient, BlueStripeCollector, NimbusWatcherService, GoogleChromeElevationService, SepMasterServiceMig, VMwareCAFCommAmqpListener, VMwareCAFManagementAgentHost, MSSQLServerADHelper, VeeamEnterpriseManagerSvc

Appendix B – EKANS Targeted Processes

Below is a list of every known process targeted by EKANS in May and June 2020.

May Variant

ccflic0.exe, ccflic4.exe, healthservice.exe, ilicensesvc.exe, nimbus.exe, prlicensemgr.exe, certificateprovider.exe, proficypublisherservice.exe, proficysts.exe, erlsrv.exe, vmtoolsd.exe, managementagenthost.exe, vgauthservice.exe, epmd.exe, hasplmv.exe, spooler.exe, hdb.exe, ntservices.exe, n.exe, monitoringhost.exe, win32sysinfo.exe, inet_gethost.exe, taskhostw.exe, proficy administrator.exe, ntevl.exe, prproficymgr.exe, prrds.exe, prrouter.exe, prconfigmgr.exe, prgateway.exe, premailengine.exe, pralarmmgr.exe, prftpengine.exe, prcalculationmgr.exe, prprintserver.exe, prdatabasemgr.exe, preventmgr.exe, prreader.exe, prwriter.exe, prsummarymgr.exe, prstubber.exe, prschedulemgr.exe, cdm.exe, musnotificationux.exe, npmdagent.exe, client64.exe, keysvc.exe, server_eventlog.exe, proficyserver.exe, server_runtime.exe, config_api_service.exe, fnplicensingservice.exe, workflowresttest.exe, proficyclient.exe, vmacthlp.exe, msdtssrvr.exe, sqlservr.exe, msmdsrv.exe, reportingservicesservice.exe, dsmcsvc.exe, winvnc4.exe, client.exe, collwrap.exe, bluestripecollector.exe, sqlbrowser.exe, dsmcad.exe, nimcluster.exe, googleupdate.exe, smc.exe, bcrservice.exe, dbsrv9.exe, rtvscan.exe, bcreporter.exe, csadmin.exe, csdbsync.exe, csmon.exe, csauth.exe, cslog.exe, csradius.exe, cstacacs.exe, url_response.exe, vmware-converter-a.exe, vmware-converter.exe, avagent.exe, paxton.net2.clientservice.exe, paxton.net2.commsserverservice.exe, avscc.exe, prunsrv.exe, googlecrashhandler.exe, googlecrashhandler64.exe, vmwaretray.exe, nd2svc.exe, tnslsnr.exe, omtsreco.exe, oracle.exe, patrolagent.exe, scfagent_64.exe, patrolperf.exe, rscdsvc.exe, rscd.exe, pmgreader.exe, firefox.exe, chrome.exe, netsession_win.exe, pcsws.exe, pcscm.exe, cwbunnav.exe, rdrcef.exe, ndrvx.exe, ndrvs.exe, dr_serviceengine.exe, teamviewer_service.exe, sqlagent.exe, dwrcst.exe, ccm messaging.exe, zoolz.exe, agntsvc.exe, dbeng50.exe, dbsnmp.exe, encsvc.exe, excel.exe, firefoxconfig.exe, infopath.exe, isqlplussvc.exe, msaccess.exe, msftesql.exe, mspub.exe, mydesktopqos.exe, mydesktopservice.exe, mysqld.exe, mysqld-nt.exe, mysqld-opt.exe, ocautoupds.exe, ocomm.exe, ocssd.exe, onenote.exe, outlook.exe, powerpnt.exe, sqbcoreservice.exe, sqlwriter.exe, steam.exe, synctime.exe, tbirdconfig.exe, thebat.exe, thebat64.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe, xfssvccon.exe, tmlisten.exe, pccntmon.exe, cntaosmgr.exe, ntrtscan.exe, mbamtray.exe, qhactivedefense.exe, qhwatchdog.exe, qhsafetray.exe, avgsvc.exe, avgui.exe, v3lite.exe, v3main.exe, v3sp.exe, avastui.exe, avastsvc.exe, avguard.exe, avshadow.exe, avgnt.exe, avira.servicehost.exe, avira.systray.exe, bdagent.exe, bdredline.exe, bdss.exe, bullguardbhvscanner.exe, bullguardscanner.exe, bullguardtray.exe, bullguardupdate.exe, bullguard.exe, cmdagent.exe, cistray.exe, cis.exe, spideragent.exe, dwengine.exe, dwarkdaemon.exe, dwnetfilter.exe, a2service.exe, a2guard.exe.a2start.exe, egui.exe, ekrn.exe, fshoster32.exe, fshoster64.exe, fortisslvpndaemon.exe, fortiesnac.exe, fortiwf.exe, fortitray.exe, fchelper64.exe, fortiproxy.exe, fcappdb.exe, fcdblog.exe, avp.exe, avpui.exe, mbamservice.exe, mcsacore.exe, mcapexe.exe, mcshield.exe, mcsvhost.exe, nortonsecurity.exe, psuaservice.exe, psuamain.exe, psanhost.exe, sdrservice.exe, swc_service.exe, swi_service.exe, ssp.exe, ccsvchst.exe, smcgui.exe, coreserviceshell.exe, coreframeworkhost.exe, uiwatchdog.exe, uiseagnt.exe, paamsrv.exe, psh_svc.exe, aupdrun.exe, acaas.exe, acaegmgr.exe, acaif.exe, acais.exe, ahnsd.exe, ahnsdsv.exe, autoup.exe, v3clnsrv.exe, v3medic.exe, v3svc.exe, aflogvw.exe, ahnrpt.exe, atwsctsk.exe, v3exec.exe, v3imscn.exe, monsvcnt.exe, monsysnt.exe, aexnsrcvsvc.exe, aexsvc.exe, atrshost.exe, ctdataload.exe, aexagentuihost.exe, aexnsagent.exe, aclntusr.exe, aexswdusr.exe, pxemtftp.exe, aclient.exe, securitycenter.exe, starta.exe, stopa.exe, anvir.exe, csrss_tc.exe, ashavast.exe, ashbug.exe, ashchest.exe, ashcmd.exe, ashdisp.exe, ashenhcd.exe, ashlogv.exe, ashmaisv.exe, ashpopwz.exe, ashquick.exe, ashserv.exe, ashsimp2.exe, ashsimpl.exe, ashskpcc.exe, ashskpck.exe, ashupd.exe, ashwebsv.exe, aswdisp.exe, aswregsvr.exe, aswserv.exe, aswupdsv.exe, aswwebsv.exe, avengine.exe, afwserv.exe, avastemupdate.exe, unsecapp.exe, avgamsvr.exe, avgas.exe, avgcc32.exe, avgcc.exe, avgctrl.exe, avgdiag.exe, avgemc.exe, avgfws8.exe, avgfwsrv.exe, avginet.exe, avgmsvr.exe, avgrssvc.exe, avgscanx.exe, avgserv9.exe, avgserv.exe, avgupd.exe, avgupdln.exe, avgupsvc.exe, avgvv.exe, avgwb.dat, avgw.exe, avgwizfw.exe, guard.exe, avgcsrvx.exe, avgidsagent.exe, avgidsmonitor.exe, avgidsui.exe, avgidswatcher.exe, avgam.exe, avgnsx.exe, avgfws9.exe, avgrsx.exe, avgtray.exe, avgwdsvc.exe, sidebar.exe, avgchsvx.exe, avgcmgr.exe, avgemcx.exe, avgfws.exe, avgmfapx.exe, avgcefrend.exe, avgcsrva.exe, avgemca.exe, avgnsa.exe, avgrsa.exe, loggingserver.exe, toolbarupdater.exe, wtusystemsuport.exe, avgregcl.exe, avgsystx.exe, vprot.exe, avcenter.exe, avconfig.exe, avesvc.exe, avmailc.exe, avmcdlg.exe, avnotify.exe, avscan.exe, guardgui.exe, avadmin.exe, avfwsvc.exe, avwebgrd.exe, fwinst.exe, sysoptenginesvc.exe, bavtray.exe, bhipssvc.exe, bmrt.exe, seccenter.exe, gziface.exe, gzserv.exe, bdc.exe, bdlite.exe, bdmcon.exe, bdsubmit.exe, deloeminfs.exe, livesrv.exe, setloadorder.exe, vsserv.exe, xcommsvr.exe, bka.exe, bkavsystemserver.exe, blupro.exe, blackd.exe, blackice.exe, proutil.exe, rapapp.exe, basfipm.exe, isafe.exe, cavrid.exe, vetmsg.exe, amswmagt, caf.exe, capmuam, agt.exe, ccnfagent.exe, ccsmagtd.exe, cfftplugin.exe, cfnotsrvd.exe, cfsmsmd.exe, alert.exe, igateway.exe, inotask.exe, caantispyware.exe, caavcmdscan.exe, caav.exe, caavguiscan.exe, cafw.exe, calogdump.exe, capfaem.exe, capfsem.exe, cappactiveprotection.exe, casecuritycenter.exe, caunst.exe, cavrep.exe, cctray.exe, ccupdate.exe, isafinst.exe, itmrt_supportdiagnostics.exe, itmrtsvc.exe, itmrt_trace.exe, ppclean.exe, umxagent.exe, umxcfg.exe, umxfwhlp.exe, umxpol.exe, unvet32.exe, capfasem.exe, ccprovsp.exe, ppctlpriv.exe, casc.exe, ccschedulersvc.exe, ccsystemreport.exe, inonmsrv.exe, inoweb.exe, auth8021x.exe, krbcc32s.exe, pep.exe, realmon.exe, repmgr64.exe, csacontrol.exe, leventmgr.exe, okclient.exe, clamscan.exe, clamtray.exe, clamwin.exe, ccemflsv.exe, cssauth.exe, cavscan.exe, clps.exe, clpsla.exe, clpsls.exe, cmdinstall.exe, cfpconfig.exe, cfp.exe, cfplogvw.exe, cfpsbmit.exe, cfpupdat.exe, crashrep.exe, cpf.exe, cfpconfg.exe, csfalconservice.exe, cylanceui.exe, cylancesvc.exe, cramtray.exe, crssvc.exe, amsvc.exe, frzstate2k.exe, drwagnui.exe, drweb32.exe, drweb32w.exe, drweb386.exe, drwebcgp.exe, drwebdc.exe, drweb.exe, drwebmng.exe, drwebscd.exe, drwebupw.exe, drwebwcl.exe, drwebwin.exe, drwinst.exe, spiderml.exe, spidernt.exe, spiderui.exe, drwagntd.exe, drwupgrade.exe, drwebcom.exe, eeyeevnt.exe, retinaengine.exe, a2guard.exe, a2start.exe, administrator.exe, control_panel.exe, usergate.exe, esmagent.exe, era.exe, ppmcativedetection.exe, vettray.exe, cavtray.exe, inorpc.exe, inort.exe, ca.exe, caissdt.exe, etagent.exe, etloganalyzer.exe, etrssfeeds.exe, evtarmgr.exe, evtmgr.exe, etreporter.exe, etconsole3.exe, etwcontrolpanel.exe, useranalysis.exe, etcorrel.exe, evtprocessecfile.exe, etscheduler.exe, useractivity.exe, traptrackermgr.exe, ewidoctrl.exe, ewidoguard.exe, nslocollectorservice.exe, fmon.exe, fortifw.exe, update_task.exe, fpavserver.exe, fprottray.exe, fameh32.exe, fspex.exe, fsaa.exe, bwgo0000, fch32.exe, fih32.exe, fsaua.exe, fsav32.exe, fscuif.exe, fsdfwd.exe, fsgk32.exe, fsgk32st.exe, fsguidll.exe, fsguiexe.exe, fshdll32.exe, fsm32.exe, fsma32.exe, fsmb32.exe, fsorsp.exe, fspc.exe, fsqh.exe, fssm32.exe, setupguimngr.exe, tnbutil.exe, fsavgui.exe, gdscan.exe, avkproxy.exe, avkservice.exe, avktray.exe, avkwctl.exe, gdfirewalltray.exe, gdfwsvc.exe, endpointsecurity.exe, esecservice.exe, gfireporterservice.exe, esecagntservice.exe, rcsvcmon.exe, dolphincharge.e, dolphincharge.exe, loggetor.exe, netalertclient.exe, printdevice.exe, pwdfilthelp.exe, pthosttr.exe, hpqwmiex.exe, ntcaagent.exe, ntcadaemon.exe, ntcaservice.exe, privacyiconclient.exe, rapuisvc.exe, vpatch.exe, tclproc.exe, isscsf.exe, issdaemon.exe, kvdetech.exe, kvmonxp_2.kxp, kvmonxp.kxp, kvolself.exe, kvsrvxp_1.exe, kvsrvxp.exe, kvxp.kxp, ppppwallrun.exe, avpcc.exe, avpexec.exe, avpm.exe, avpncc.exe, avps.exe, avpupd.exe, kav.exe, kavisarv.exe, kavmm.exe, kavss.exe, kavsvc.exe, kis.exe, klnagent.exe, klswd.exe, klwtblfs.exe, kwsprod.exe, up2date.exe, klserver.exe, oespamtest.exe, kavadapterexe.exe, kavlotsingleton.exe, kavfsgt.exe, kavfsrcn.exe, kavfs.exe, kavfswp.exe, kavshell.exe, klnacserver.exe, avpdtagt.exe, netcfg.exe, kavfsscs.exe, kavtray.exe, persfw.exe, avserver.exe, winroute.exe, wrctrl.exe, kabackreport.exe, kaccore.exe, kanmcmain.exe, kastray.exe, kislive.exe, kmailmon.exe, knupdatemain.exe, kswebshield.exe, kxeserv.exe, uplive.exe, kansgui.exe, kansvr.exe, kavstart.exe, kpfwsvc.exe, kwatch.exe, kav32.exe, kissvc.exe, kpfw32.exe, system.exe, wssfcmai.exe, aawservice.exe, ad-aware2007.exe, nlsvc.exe, engineserver.exe, eventparser.exe, log_qtine.exe, mfeann.exe, nailgpip.exe, rpcserv.exe, srvmon.exe, mcagent.exe, mfemactl.exe, macmnsvc.exe, masvc.exe, masalert.exe, msssrv.exe, massrv.exe, msscli.exe, mcshld9x.exe, mgavrtcl.exe, mcappins.exe, mfecanary.exe, macompatsvc.exe, mcvsrte.exe, mfefire.exe, dao_log.exe, firesvc.exe, firetray.exe, mfeesp.exe, naprdmgr.exe, cpd.exe, mfefw.exe, frameworkservic, cmgrdian.exe, mcshell.exe, mfehcs.exe, mcinfo.exe, hwapi.exe, mcafeedatabackup.exe, mcmscsvc.exe, mcnasvc.exe, mcods.exe, mcpromgr.exe, mcproxy.exe, mcuimgr.exe, mpfsrv.exe, mpsevh.exe, mps.exe, msksrver.exe, redirsvc.exe, saservice.exe, siteadv.exe, mfemms.exe, neotrace.exe, vshwin32.exe, mpfagent.exe, mpfconsole.exe, mpf.exe, mpfservice.exe, mpftray.exe, mscifapp.exe, mfevtps.exe, qclean.exe, mcregwiz.exe, rssensor.exe, safeservice.exe, ncdaemon.exe, mcdash.exe, mcdetect.exe, sssscheduler.exe, sahookmain.exe, mskdetct.exe, msksrvr.exe, mskagent.exe, stinger.exe, mcsysmon.exe, mctskshd.exe, mfetp.exe, myagttry.exe, mcupdmgr.exe, rulaunch.exe, mcvsshld.exe, tbmon.exe, alogserv.exe, mcmnhdlr.exe, mghtml.exe, edisk.exe, scan32.exe, frameworkservice.exe, mcconsol.exe, mcscript_inuse.exe, mctray.exe, mcupdate.exe, shstat.exe, udaterui.exe, updaterui.exe, mcepoc.exe, mcepocfg.exe, mcpalmcfg.exe, mcwcecfg.exe, mcwce.exe, frameworkservic.exe, vsmain.exe, oasclnt.exe, vsstat.exe, mcvsftsn.exe, avconsol.exe, avsynmgr.exe, vstskmgr.exe, webscanx.exe, mfewc.exe, mfewch.exe, giantantispywaremain.exe, giantantispywareupdater.exe, gcasservalert.exe, gcascleaner.exe, gcasinstallhelper.exe, gcasnotice.exe, gcasdtserv.exe, gcasserv.exe, gcasswupdater.exe, fcsms.exe, fcssas.exe, nissrv.exe, dpmra.exe, msseces.exe, wscntfy.exe, securitymanager.exe, aesecurityservice.exe, deteqt.agent.exe, omniagent.exe, nerosvc.exe, seanalyzertool.exe, spyemergency.exe, spyemergencysrv.exe, nlclient.exe, crdm.exe, nmagent.exe, ehttpsrv.exe, nod32.exe, nod32krn.exe, nod32kui.exe, nod32view.exe, cclaw.exe, elogsvc.exe, nip.exe, nipsvc.exe, njeeves.exe, npfmsg2.exe, npfmsg.exe, npfsvice.exe, nrmenctb.exe, nvcoas.exe, nvcsched.exe, nymse.exe, zanda.exe, zlh.exe, ixaptsvc.exe, ixavsvc.exe, ixfwsvc.exe, emlproui.exe, emlproxy.exe, mpsvc.exe, onlinent.exe, onlnsvc.exe, scanmsg.exe, scanwscs.exe, tsansrf.exe, tsatisy.exe, tscutynt.exe, tsmpnt.exe, upschd.exe, xfilter.exe, aps.exe, aus.exe, outpost.exe, adminserver.exe, avtask.exe, clshield.exe, console.exe, cpntsrv.exe, padfsvr.exe, pasystemtray.exe, pavfnsvr.exe, pavkre.exe, pavprot.exe, pavreport.exe, pnmsrv.exe, psimsvc.exe, pavupg.exe, remupd.exe, iface.exe, pavfires.exe, pavmail.exe, pavprsrv.exe, pavsched.exe, pavsrv50.exe, pavsrv51.exe, pavsrv52.exe, prevsrv.exe, tpsrv.exe, pagent.exe, pagentwd.exe, psctris.exe, apvxdwin.exe, inicio.exe, pavbckpt.exe, pavjobs.exe, psctrls.exe, pshost.exe, psimreal.exe, pskmssvc.exe, srvload.exe, webproxy.exe, avltmain.exe, firewallgui.exe, pviewer.exe, pview.exe, pmon.exe, qoeloader.exe, fws.exe, ccenter.exe, ravxp.exe, rfwproxy.exe, rfwstub.exe, knownsvr.exe, ras.exe, rasupd.exe, upfile.exe, rstray.exe, ravalert.exe, rav.exe, ravmond.exe, ravmon.exe, ravservice.exe, ravstub.exe, ravtask.exe, ravtray.exe, ravupdate.exe, rnreport.exe, rsnetsvr.exe, scanfrm.exe, rfwmain.exe, rfwsrv.exe, winlog.exe, omslogmanager.exe, snhwsrv.exe, snicheckadm.exe, snichecksrv.exe, snicon.exe, snsrv.exe, smsx.exe, svcharge.exe, svdealer.exe, svframe.exe, svtray.exe, sschk.exe, trjscan.exe, trupd.exe, ssecuritymanager.exe, dltray.exe, dlservice.exe, almon.exe, lmon.exe, savadminservice.exe, savservice.exe, sweepsrv.sys, swnetsup.exe, alsvc.exe, alupdate.exe, savmain.exe, sav32cli.exe, certificationmanagerservicent.exe, emlibupdateagentnt.exe, managementagentnt.exe, mgntsvc.exe, routernt.exe, schdsrvc.exe, scfmanager.exe, scfservice.exe, scftray.exe, op_viewer.exe, sgbhp.exe, pctsauxs.exe, pctsgui.exe, pctssvc.exe, pctstray.exe, regmech.exe, sdtrayapp.exe, svcntaux.exe, swdsvc.exe, swnxt.exe, execstat.exe, seestat.exe, swserver.exe, slee81.exe, kpf4gui.exe, kpf4ss.exe, wrspysetup.exe, acctmgr.exe, alertsvc.exe, alunotify.exe, aluschedulersvc.exe, appsvc32.exe, ccap.exe, ccapp.exe, ccevtmgr.exe, ccproxy.exe, ccpxysvc.exe, ccsetmgr.exe, checkup.exe, cka.exe, comhost.exe, cpdclnt.exe, csinject.exe, csinsm32.exe, csinsmnt.exe, dbserv.exe, defwatch.exe, defwatch, diskmon.exe, djsnetcn.exe, doscan.exe, dwhwizrd.exe, fwcfg.exe, ghost_2.exe, ghosttray.exe, icepack.exe, idsinst.exe, ispwdsvc.exe, issvc.exe, isuac.exe, luall.exe, lucallbackproxy.exe, lucoms~1.exe, lucoms.exe, mcui32.exe, navapsvc.exe, navapw32.exe, navectrl.exe, navelog.exe, navesp.exe, navshcom.exe, navw32.exe, navwnt.exe, ndetect.exe, ngctw32.exe, ngserver.exe, nisoptui.exe, nisserv.exe, nisum.exe, nmain.exe, npfmntor.exe, nprotect.exe, npscheck.exe, npssvc.exe, nscsrvce.exe, nsctop.exe, nsmdtr.exe, olfsnt40.exe, opscan.exe, poproxy.exe, pqibrowser.exe, pqv2isvc.exe, pxeservice.exe, qdcsfs.exe, qserver.exe, reportersvc.exe, rnav.exe, savfmsesp.exe, savroam.exe, savscan.exe, savui.exe, sbserv.exe, scan, explicit.exe, semsvc.exe, sesclu.exe, sevinst.exe, smsectrl.exe, smselog.exe, smsesjm.exe, smsesp.exe, smsesrv.exe, smsetask.exe, smseui.exe, sms.exe, sndmon.exe, sndsrvc.exe, spbbcsvc.exe, symlcsvc.exe, symproxysvc.exe, symsport.exe, symtray.exe, symwsc.exe, sysdoc32.exe, ucservice.exe, updtnv28.exe, urllstck.exe, usrprmpt.exe, v2iconsole.exe, vpc32.exe, vpdn_lu.exe, vprosvc.exe, wfxctl32.exe, wfxmod32.exe, wfxsnt40.exe, lucomserver.exe, savfmselog.exe, savfmsesjm.exe, savfmsectrl.exe, savfmsespamstatsmanager.exe, savfmsesrv.exe, savfmsetask.exe, savfmseui.exe, snac.exe, ssm.exe, reportsvc.exe, vptray.exe, procexp.exe, tdimon.exe, tfun.exe, tfgui.exe, tfservice.exe, tftray.exe, tiaspn~1.exe, traflnsp.exe, asupport.exe, isntsmtp.exe, nsmdemf.exe, nsmdmon.exe, nsmdreal.exe, nsmdsch.exe, ofcdog.exe, pccnt.exe, pccntupd.exe, pcctlcom.exe, pcscnsrv.exe, schupd.exe, tmntsrv.exe, tmpfw.exe, tmproxy.exe, tmas.exe, entitymain.exe, aphost.exe, lwdmserver.exe, mrf.exe, isntsysmonitor, ofcpfwsvc.exe, dwwin.exe, patch.exe, pccclient.exe, pccguide.exe, pcclient.exe, pccpfw.exe, pcscan.exe, pntiomon.exe, pop3pack.exe, pop3trap.exe, scanmailoutlook.exe, smoutlookpack.exe, webtrapnt.exe, euqmonitor.exe, smex_activeupda, smex_master.exe, smex_remoteconf, smex_systemwatc, svcgenerichost, spntsvc.exe, stopp.exe, stwatchdog.exe, usbguard.exe, uploadrecord.exe, sbamsvc.exe, vrvmail.exe, vrvmon.exe, vrvnet.exe, vrv.exe, wrsa.exe, networkagent.exe, websensecontrolservice.exe, mpcmdrun.exe, msascui.exe, msmpeng.exe, mspmspsv.exe, kb891711.exe, zavaux.exe, zavcore.exe, zillya.exe, zlclient.exe, vsmon.exe, forcefield.exe, iswmgr.exe, zapro.exe, zonealarm.exe, mantispm.exe, GDDServer.exe

June Variant

avsynmgr.exe, vstskmgr.exe, webscanx.exe, c.exe, ch.exe, gcascleaner.exe, gcasnotice.exe, gcasdtserv.exe, gcasserv.exe, fcsms.exe, fcssas.exe, nissrv.exe, dpmra.exe, msseces.exe, wscntfy.exe, deteqt.agent.exeomniagent.exe, nerosvc.exe, spyemergency.exenlclient.exe, crdm.exenip.exe, nmagent.exe, ehttpsrv.exe, nod32.exe, nod32krn.exe, nod32kui.exe, nod32view.exe, cclaw.exe, elogsvc.exe, nipsvc.exe, njeeves.exe, npfmsg2.exe, npfmsg.exe, npfsvice.exe, nrmenctb.exe, nvcoas.exe, nvcsched.exe, nymse.exezlh.exezanda.exe, ixaptsvc.exe, ixavsvc.exe, ixfwsvc.exe, emlproui.exe, emlproxy.exe, mpsvc.exeaps.exeonlinent.exe, onlnsvc.exe, scanmsg.exe, scanwscs.exe, tsansrf.exe, tsatisy.exe, tscutynt.exe, tsmpnt.exe, upschd.exe, xfilter.exe, aus.exeiface.exeoutpost.exe, adminserver.exe, avtask.exe, clshield.exe, console.exe, cpntsrv.exe, padfsvr.exe, pasystemtray.exepavfnsvr.exe, pavkre.exe, pavprot.exe, pavreport.exe, pnmsrv.exe, psimsvc.exe, pavupg.exe, remupd.exe, pavfires.exe, pavmail.exe, pavprsrv.exe, pavsched.exe, pavsrv50.exe, pavsrv51.exe, pavsrv52.exe, prevsrv.exe, tpsrv.exe, pagent.exe, pagentwd.exe, psctris.exe, apvxdwin.exe, inicio.exe, pavbckpt.exe, pavjobs.exe, psctrls.exe, pshost.exe, psimreal.exe, pskmssvc.exe, srvload.exe, webproxy.exe, avltmain.exe, firewallgui.exe, pviewer.exe, pview.exe, pmon.exefws.exe, qoeloader.exe, ccenter.exe, ravxp.exeras.exerfwproxy.exe, rfwstub.exe, knownsvr.exe, rasupd.exe, upfile.exe, rstray.exe, ravalert.exe, rav.exesnsrv.exeravmond.exe, ravmon.exe, ravservice.exe, ravstub.exe, ravtask.exe, ravtray.exe, ravupdate.exe, rnreport.exe, rsnetsvr.exe, scanfrm.exe, rfwmain.exe, rfwsrv.exe, winlog.exe, snhwsrv.exe, snicheckadm.exe, snichecksrv.exe, snicon.exe, smsx.exelmon.exesvcharge.exe, svdealer.exe, svframe.exe, svtray.exe, sschk.exe, trjscan.exe, trupd.exe, dltray.exe, dlservice.exe, almon.exe, savservice.exe, sweepsrv.sys, swnetsup.exe, alsvc.exe, alupdate.exe, savmain.exe, sav32cli.exe, mgntsvc.exe, routernt.exe, schdsrvc.exe, scfmanager.exe, scfservice.exe, scftray.exe, op_viewer.exe, sgbhp.exe, pctsauxs.exe, pctsgui.exe, pctssvc.exe, pctstray.exe, regmech.exe, sdtrayapp.exe, svcntaux.exe, swdsvc.exe, swnxt.exe, execstat.exe, seestat.exe, swserver.exe, slee81.exe, kpf4gui.exe, kpf4ss.exe, wrspysetup.exe, acctmgr.exe, alertsvc.exe, alunotify.exe, appsvc32.exe, ccap.execka.exe, ccapp.exe, ccevtmgr.exe, ccproxy.exe, ccpxysvc.exe, ccsetmgr.exe, checkup.exe, comhost.exe, cpdclnt.exe, csinject.exe, csinsm32.exe, csinsmnt.exe, dbserv.exe, defwatch.exe, defwatchrnav.exediskmon.exe, djsnetcn.exe, doscan.exe, dwhwizrd.exe, fwcfg.exe, ghost_2.exe, ghosttray.exe, icepack.exe, idsinst.exe, ispwdsvc.exe, issvc.exe, isuac.exe, luall.exe, lucoms.exe, mcui32.exe, navapsvc.exe, navapw32.exe, navectrl.exe, navelog.exe, navesp.exe, navshcom.exe, navw32.exe, navwnt.exe, ndetect.exe, ngctw32.exe, ngserver.exe, nisoptui.exe, nisserv.exe, nisum.exe, nmain.exe, npfmntor.exe, nprotect.exe, npscheck.exe, npssvc.exe, nscsrvce.exe, nsctop.exe, nsmdtr.exe, olfsnt40.exe, opscan.exe, poproxy.exe, pqibrowser.exe, pqv2isvc.exe, pxeservice.exe, qdcsfs.exe, qserver.exe, reportersvc.exe, savfmsesp.exe, savroam.exe, savscan.exe, savui.exe, scansbserv.exe, explicit.exe, semsvc.exe, sesclu.exe, sevinst.exe, smsectrl.exe, smselog.exe, smsesjm.exe, smsesp.exe, smsesrv.exe, smsetask.exe, smseui.exe, sms.exevpc32.exesndmon.exe, sndsrvc.exe, spbbcsvc.exe, symlcsvc.exe, symproxysvc.exe, symsport.exe, symtray.exe, symwsc.exe, sysdoc32.exe, ucservice.exe, updtnv28.exe, urllstck.exe, usrprmpt.exe, v2iconsole.exe, vpdn_lu.exe, vprosvc.exe, wfxctl32.exe, wfxmod32.exe, wfxsnt40.exe, lucomserver.exe, savfmselog.exe, savfmsesjm.exe, savfmsectrl.exe, savfmsesrv.exe, savfmsetask.exe, savfmseui.exe, snac.exessm.exe, reportsvc.exe, vptray.exe, procexp.exe, tdimon.exe, tfun.exetmas.exetfgui.exe, tfservice.exe, tftray.exe, traflnsp.exe, asupport.exe, isntsmtp.exe, nsmdemf.exe, nsmdmon.exe, nsmdreal.exe, nsmdsch.exe, ofcdog.exe, pccnt.exe, pccntupd.exe, pcctlcom.exe, pcscnsrv.exe, schupd.exe, tmntsrv.exe, tmpfw.exe, tmproxy.exe, entitymain.exe, aphost.exe, lwdmserver.exe, mrf.exedwwin.exeisntsysmonitor, fcpfwsvc.exe, patch.exevrv.exepccclient.exe, pccguide.exe, pcclient.exe, pccpfw.exe, pcscan.exe, pntiomon.exe, pop3pack.exe, pop3trap.exe, webtrapnt.exe, euqmonitor.exe, smex_activeupda, smex_master.exe, smex_remoteconf, smex_systemwatc, svcgenerichost, spntsvc.exe, stopp.exe, stwatchdog.exe, usbguard.exe, uploadrecord.exesbamsvc.exe, vrvmail.exe, vrvmon.exe, vrvnet.exe, wrsa.exexagt.exenetworkagent.exempcmdrun.exe, msascui.exe, msmpeng.exe, mspmspsv.exe, kb891711.exe, zavaux.exe, zavcore.exe, thebat.exe, thebat64.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe, xfssvccon.exe, tmlisten.exe, pccntmon.exe, cntaosmgr.exe, ntrtscan.exe, mbamtray.exe, qhwatchdog.exe, qhsafetray.exe, avgsvc.exe, avgui.exe, v3lite.exe, v3main.exe, avastui.exe, avastsvc.exe, avguard.exe, avshadow.exe, avgnt.exe, bdagent.exe, bdredline.exe, bdss.execis.exe, bullguard.exe, cmdagent.exe, cistray.exe, spideragent.exe, dwengine.exe, dwarkdaemon.exe, dwnetfilter.exe, a2service.exe, egui.exeekrn.exefshoster32.exe, fshoster64.exe, fortiesnac.exe, fortiwf.exe, fortitray.exe, fchelper64.exe, fortiproxy.exe, fcappdb.exe, fcdblog.exe, avp.exeavpui.exembamservice.exe, mcsacore.exe, mcapexe.exe, mcshield.exe, mcsvhost.exe, psuaservice.exe, psuamain.exe, psanhost.exe, sdrservice.exe, swc_service.exe, swi_service.exe, ssp.exeacaas.execcsvchst.exe, smcgui.exe, uiwatchdog.exe, uiseagnt.exe, paamsrv.exe, psh_svc.exe, aupdrun.exe, acaegmgr.exe, acaif.exe, acais.exe, ahnsd.exe, ahnsdsv.exe, autoup.exe, v3clnsrv.exe, v3medic.exe, v3svc.exe, aflogvw.exe, ahnrpt.exe, atwsctsk.exe, v3exec.exe, v3imscn.exe, monsvcnt.exe, monsysnt.exe, aexnsrcvsvc.exe, aexsvc.exe, atrshost.exe, ctdataload.exe, aexnsagent.exe, aclntusr.exe, aexswdusr.exe, pxemtftp.exe, aclient.exe, starta.exe, stopa.exe, anvir.exe, csrss_tc.exe, ashavast.exe, ashbug.exe, ashchest.exe, ashcmd.exe, ashdisp.exe, ashenhcd.exe, ashlogv.exe, ashmaisv.exe, ashpopwz.exe, ashquick.exe, ashserv.exe, ashsimp2.exe, ashsimpl.exe, ashskpcc.exe, ashskpck.exe, ashupd.exe, ashwebsv.exe, aswdisp.exe, aswregsvr.exe, aswserv.exe, aswupdsv.exe, aswwebsv.exe, avengine.exe, afwserv.exe, unsecapp.exe, avgamsvr.exe, avgas.exe, avgcc32.exe, avgcc.exe, avgctrl.exe, avgdiag.exe, avgemc.exe, avgfws8.exe, avgfwsrv.exe, avginet.exe, avgmsvr.exe, avgrssvc.exe, avgscanx.exe, avgserv9.exe, avgserv.exe, avgupd.exe, avgupdln.exe, avgupsvc.exe, avgvv.exe, avgwb.dat, avgw.exebmrt.exeavgwizfw.exe, guard.exe, avgcsrvx.exe, avgidsagent.exe, avgidsui.exe, avgam.exe, avgnsx.exe, avgfws9.exe, avgrsx.exe, avgtray.exe, avgwdsvc.exe, sidebar.exe, avgchsvx.exe, avgcmgr.exe, avgemcx.exe, avgfws.exe, avgmfapx.exe, avgcefrend.exe, avgcsrva.exe, avgemca.exe, avgnsa.exe, avgrsa.exe, avgregcl.exe, avgsystx.exe, vprot.exe, avcenter.exe, avconfig.exe, avesvc.exe, avmailc.exe, avmcdlg.exe, avnotify.exe, avscan.exe, guardgui.exe, avadmin.exe, avfwsvc.exe, avwebgrd.exe, fwinst.exe, bavtray.exe, bhipssvc.exe, seccenter.exe, gziface.exe, gzserv.exe, bdc.exebka.exe, bdlite.exe, bdmcon.exe, bdsubmit.exe, deloeminfs.exe, livesrv.exe, setloadorder.exevsserv.exe, xcommsvr.exe, blupro.exe, blackd.exe, blackice.exe, proutil.exe, rapapp.exe, basfipm.exe, isafe.exe, cavrid.exe, vetmsg.exe, amswmagtcaf.exe, capmuamagt.exe, ccnfagent.exe, ccsmagtd.exe, cfftplugin.exe, cfnotsrvd.exe, cfsmsmd.exe, alert.exe, igateway.exe, inotask.exe, caavcmdscan.exe, caav.execafw.execaavguiscan.exe, calogdump.exe, capfaem.exe, capfsem.exe, caunst.exe, cavrep.exe, cctray.exe, ccupdate.exe, isafinst.exe, itmrtsvc.exe, itmrt_trace.exe, ppclean.exe, umxagent.exe, umxcfg.exe, umxfwhlp.exe, umxpol.exe, unvet32.exe, capfasem.exe, ccprovsp.exe, ppctlpriv.exe, casc.exepep.exe, inonmsrv.exe, inoweb.exe, auth8021x.exe, krbcc32s.exe, realmon.exe, repmgr64.exe, csacontrol.exe, leventmgr.exe, okclient.exe, clamscan.exe, clamtray.exe, clamwin.exe, ccemflsv.exe, cssauth.exe, cavscan.exe, clps.execfp.exe, clpsla.exe, clpsls.exe, cmdinstall.exe, cfpconfig.exe, cfplogvw.exe, cfpsbmit.exe, cfpupdat.exe, crashrep.exe, cpf.exeamsvc.execfpconfg.exe, cylanceui.exe, cylancesvc.exe, cramtray.exe, crssvc.exe, frzstate2k.exe, drwagnui.exe, drweb32.exe, drweb32w.exe, drweb386.exe, drwebcgp.exe, drwebdc.exe, drweb.exeera.exedrwebmng.exe, drwebscd.exe, drwebupw.exe, drwebwcl.exe, drwebwin.exe, drwinst.exe, spiderml.exe, spidernt.exe, spiderui.exe, drwagntd.exe, drwupgrade.exe, drwebcom.exe, eeyeevnt.exe, retinaengine.exea2guard.exe, a2start.exe, usergate.exe, esmagent.exe, vettray.exe, cavtray.exe, inorpc.exe, inort.exe, ca.execaissdt.exe, etagent.exe, etrssfeeds.exe, evtarmgr.exe, evtmgr.exe, etreporter.exe, etconsole3.exe, useranalysis.exeetcorrel.exe, etscheduler.exe, useractivity.exeewidoctrl.exe, ewidoguard.exe, fmon.exefsaa.exefortifw.exe, update_task.exe, fpavserver.exe, fprottray.exe, fameh32.exe, fspex.exe, bwgo0000fspc.exefch32.exe, fih32.exe, fsaua.exe, fsav32.exe, fscuif.exe, fsdfwd.exe, fsgk32.exe, fsgk32st.exe, fsguidll.exe, fsguiexe.exe, fshdll32.exe, fsm32.exe, fsma32.exe, fsmb32.exe, fsorsp.exe, fsqh.exekvxp.kxpfssm32.exe, setupguimngr.exetnbutil.exe, fsavgui.exe, gdscan.exe, avkproxy.exe, avkservice.exe, avktray.exe, avkwctl.exe, gdfwsvc.exe, esecservice.exe, rcsvcmon.exe, dolphincharge.e, loggetor.exe, printdevice.exe, pwdfilthelp.exe, pthosttr.exe, hpqwmiex.exe, ntcaagent.exe, ntcadaemon.exe, ntcaservice.exe, rapuisvc.exe, vpatch.exe, tclproc.exe, isscsf.exe, issdaemon.exe, kvdetech.exe, kvmonxp_2.kxp, kvmonxp.kxp, kvolself.exe, kvsrvxp_1.exe, kvsrvxp.exe, ppppwallrun.exe, avpcc.exe, avpexec.exe, avpm.exeavps.exeavpncc.exe, avpupd.exe, kav.exekavmm.exekavisarv.exe, kavss.exekis.exekavsvc.exe, klnagent.exe, klswd.execpd.exeklwtblfs.exe, kwsprod.exe, up2date.exe, klserver.exe, oespamtest.exe, kavfsgt.exe, kavfsrcn.exe, kavfs.exe, kavfswp.exe, kavshell.exe, klnacserver.exe, avpdtagt.exe, netcfg.exe, kavfsscs.exe, kavtray.exe, persfw.exe, avserver.exe, winroute.exe, wrctrl.exe, kabackreport.exekaccore.exe, kanmcmain.exe, kastray.exe, kislive.exe, kmailmon.exe, knupdatemain.exekswebshield.exe, kxeserv.exe, uplive.exe, kansgui.exe, kansvr.exe, kavstart.exe, kpfwsvc.exe, kwatch.exe, kav32.exe, kissvc.exe, kpfw32.exe, system.exe, wssfcmai.exe, aawservice.exe, engineserver.exeeventparser.exe, log_qtine.exe, mfeann.exe, nailgpip.exe, rpcserv.exe, srvmon.exe, mcagent.exe, mfemactl.exe, macmnsvc.exe, masvc.exe, masalert.exe, msssrv.exe, massrv.exe, msscli.exe, mcshld9x.exe, mgavrtcl.exe, mcappins.exe, mfecanary.exe, macompatsvc.exe, mcvsrte.exe, mfefire.exe, dao_log.exe, firesvc.exe, firetray.exe, mfeesp.exe, naprdmgr.exe, mfefw.exemps.exeframeworkservic, cmgrdian.exe, mcshell.exe, mfehcs.exe, mcinfo.exe, hwapi.exe, mcmscsvc.exe, mcnasvc.exe, mcods.exe, mcpromgr.exe, mcproxy.exe, mcuimgr.exe, mpfsrv.exe, mpsevh.exe, msksrver.exe, redirsvc.exe, saservice.exe, siteadv.exe, mfemms.exe, neotrace.exe, vshwin32.exe, mpfagent.exe, mpfconsole.exe, mpf.exemfetp.exempfservice.exe, mpftray.exe, mscifapp.exe, mfevtps.exe, qclean.exe, mcregwiz.exe, rssensor.exe, safeservice.exe, ncdaemon.exe, mcdash.exe, mcdetect.exe, ssscheduler.exe, sahookmain.exe, mskdetct.exe, msksrvr.exe, mskagent.exe, stinger.exe, mcsysmon.exe, mctskshd.exe, myagttry.exe, mcupdmgr.exe, rulaunch.exe, mcvsshld.exe, tbmon.exe, alogserv.exe, mcmnhdlr.exe, mghtml.exe, edisk.exe, scan32.exe, mcconsol.exe, mctray.exe, mcupdate.exe, shstat.exe, udaterui.exe, updaterui.exe, mcepoc.exe, mcepocfg.exe, mcpalmcfg.exe, mcwcecfg.exe, mcwce.exe, vsmain.exe, oasclnt.exe, vsstat.exe, mcvsftsn.exe, avconsol.exe, kavlotsingleton.exe, mcafeedatabackup.exe, frameworkservice.exe, mcscript_inuse.exe, frameworkservic.exe, giantantispywaremain.exe, giantantispywareupdater.exe, gcasservalert.exe, gcasinstallhelper.exe, gcasswupdater.exe, securitymanager.exe, aesecurityservice.exe, seanalyzertool.exe, spyemergencysrv.exe, omslogmanager.exe, ssecuritymanager.exe, savadminservice.exe, emlibupdateagentnt.exe, managementagentnt.exe, aluschedulersvc.exe, lucallbackproxy.exe, savfmsespamstatsmanager.exe, scanmailoutlook.exe, smoutlookpack.exe, websensecontrolservice.exe

Appendix C – Targeted Extensions for Both EKANS Variants

.docx, .accdb, .accde, .accdr, .accdt, .asp, .aspx, .back, .backup, .backupdb, .bak, .mdb, .mdc, .mdf, .war, .xls, .xlsx, .xlsm, .xlr, .zip, .rar, .sqlitedb, .sql, .py, .ppam, .pps, .ppsm, .ppsx, .ppt, pptm, .pptx, .hpp, .java, .jsp, .php, .doc, .docm, .pst, .psd, .dot, dotm, .cpp, .cs, .csv, .bkp, .db, .db-journal, .csproj, .sln, .md, .pl, .js, .html, .htm, .dbf, .rdo, .arc, .vhd, .vmdk, .vdi, .vhdx, .edb, .c, .h

FortiGuard Labs has shared the findings of this research analysis with fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit cyberthreatalliance.org.

Learn more about FortiGuard Labs threat research and the FortiGuard Security Subscriptions and Services portfolio. Sign up for the weekly Threat Brief from FortiGuard Labs.

Related Posts

Copyright © 2022 Fortinet, Inc. All Rights Reserved