GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Tuesday, December 4, 2018
GLESEC-CSFR0037

Malware Analysis Report (AR18-337A)

MAR-10219351.r1.v2 – SamSam1

Original release date: December 03, 2018

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp.

Summary

Description

Two (2) artifacts were submitted for analysis. The analysis indicates that these files are ransomware.

For a downloadable copy of IOCs, see:

- MAR-10219351.r1.v2.stix

Submitted Files (2)

5d65ebdde1aef8f23114f95454287e7410965288f144d880ece2a2b8c3128645 (prelecturedexe.exe)

d8d919d884b86e4d5977598bc9d637ed53e21d5964629d0427077e08ddbcba68 (proteusdlll.dll)

Findings

5d65ebdde1aef8f23114f95454287e7410965288f144d880ece2a2b8c3128645

Tags

ransomwaretrojan

Details

Name	prelecturedexe.exe

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Size	1024512 bytes
Type	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	222d7fde37ae344824a97087d473cdcd
SHA1	90205a2761ed7ac3b188230786ec2bebd30effba
SHA256	5d65ebdde1aef8f23114f95454287e7410965288f144d880ece2a2b8c3128645
SHA512	177f25c2e454b5366719a5536e25dbf16ab5cb01b1886b18ea1477671651191cbf663cf1754990c618
ssdeep	24576:PLvqxk7+y/4NmWPWKrbE6qqE56Hglx8zudJhTyGwcKe:+
Entropy	4.695794

Antivirus

Ahnlab	Trojan/Win32.MSILKrypt
Antiy	Trojan/Win32.Dynamer
Avira	TR/Runner.egvkh
BitDefender	Gen:Variant.Kazy.368437
Cyren	W32/Trojan.XCIK-1629
ESET	a variant of MSIL/Runner.N trojan
Emsisoft	Gen:Variant.Kazy.368437 (B)
Ikarus	Trojan.MSIL.Runner
K7	Trojan (0053adaa1)
McAfee	Generic.dyp
Microsoft Security Essentials	Trojan:MSIL/Runner
Quick Heal	Trojan.IGENERIC
Sophos	Mal/Kryptik-BV
Symantec	Trojan.Gen.2
Zillya!	Trojan.Runner.Win32.876

Yara Rules

No matches found.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-09-16 03:31:51-04:00
Import Hash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

MD5	Name	Raw Size	Entropy
5e1317af9956be12deebdea49aae14f5	header	512	2.723403
124120a6b861fdfff756e19a77a53e05	.text	1020928	4.695157
8a2d72fec9d2535440e0f83b59253f2b	.rsrc	2560	3.722300
b227291feae10a83e762c2bc9d959a7f	.reloc	512	0.101910

Packers/Compilers/Cryptors

Microsoft Visual C# v7.0 / Basic .NET

Process List

Process	PID	PPID
lsass.exe	488	(388)
5d65ebdde1aef8f23114f95454287e7410965288f144d880ece2a2b8c3128645.exe	1976	(2556)
dw20.exe	1936	(1976)

Relationships

5d65ebdde1...	Related_To	d8d919d884b86e4d5977598bc9d637ed53e21d5964629d0427077e08ddbcba68

Description

This file is a 32-bit Windows executable. The file has been identified as ransomware written in C Sharp (C#). It contains a namespace named "prelecturedexe" and a class named "Program."

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

This ransomware is invoked using the following command-line format:

-- Begin command format --

prelecturedexe.exe <argv0> <argv1> <argv2> <argv3>

-- End command format --

The execution will quit if 4 arguments are not used.

This ransomware uses Advanced Encryption Standard (AES) encryption. When executed, it uses a command-line argument <argv0> as a component for the AES Rijndael Key and initialization vector (IV). <argv1> <argv2> <argv3> are files and directories to be encrypted/decrypted.

It reads a file named "*.nike2018" in the same directory where this executable resides. If the file "*.nike2018" does not exist, the execution quits. It removes "*.nike2018" after it reads the file content.

d8d919d884b86e4d5977598bc9d637ed53e21d5964629d0427077e08ddbcba68

Tags

ransomwaretrojan

Details

Name	proteusdlll.dll
Size	409600 bytes
Type	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	fe3ae84a8defc809e734bbd0736f82de
SHA1	04a2ea4c78f78d628800c0a5cb9547a0c0b14378
SHA256	d8d919d884b86e4d5977598bc9d637ed53e21d5964629d0427077e08ddbcba68
SHA512	9cb6ddb8a0b9329fe08fcf8a02d45c43222432d6e145f55deacb019f772970513d3ddfa589a002c0abf
ssdeep	3072:Sa6J+OIazQ94ZPaqa7YHmIZwUSToQemTIC6:A+OIa094ZPRakH/+USE
Entropy	4.645654

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Antivirus

Ahnlab	Trojan/Win32.MSILKrypt
Antiy	Trojan/MSIL.Runner
Avira	TR/Runner.pjtvf
BitDefender	Gen:Variant.Ursu.265937
ClamAV	Win.Ransomware.Samsam-6482588-0
Cyren	W32/Trojan.NADV-8499
ESET	a variant of MSIL/Runner.N trojan
Emsisoft	Gen:Variant.Ursu.265937 (B)
Ikarus	Trojan.MSIL.Runner
K7	Trojan (0053adaa1)
McAfee	RDN/Generic.dx
Microsoft Security Essentials	Trojan:MSIL/Runner
Quick Heal	Trojan.IGENERIC
Sophos	Troj/Kryptik-IS
Symantec	Trojan.Gen.2
Zillya!	Trojan.Runner.Win32.880

Yara Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-09-16 03:31:51-04:00
Import Hash	dae02f32a21e03ce65412f6e56942daa

PE Sections

MD5	Name	Raw Size	Entropy

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

397b763d106b2f347c5a563922273551	header	512	2.714618
ad25e96cae2016331129ec4643535822	.text	406528	4.650477
01784b876d14b1384491318f8fce07d5	.rsrc	2048	2.987471
816849886aa28e56db0cd065fae38897	.reloc	512	0.101910

Packers/Compilers/Cryptors

Microsoft Visual C# / Basic .NET

Process List

Process	PID	PPID
lsass.exe	488	(384)
rundll32.exe	3028	(2984)

Relationships

d8d919d884...	Related_To	5d65ebdde1aef8f23114f95454287e7410965288f144d880ece2a2b8c3128645

Description

This dynamic link library (DLL) contains functions used by the ransomware "prelecturedexe.exe" (222d7fde37ae344824a97087d473cdcd).

It contains a namespace named "proteusdlll" and a class named "Class1."

It contains functions to generate the AES Rijndael Key and IV, function to create the Rijndael decryptor and function to encrypt/decrypt victim's files.

The AES Rijndael Key and IV is generated from the following predefined bytes and the first command line argument <argv0>.

-- Begin predefined bytes to generate Rijndael Key and IV --

0x49
0x76
0x61

0x6E
0x20
0x4D
0x65
0x64
0x76
0x65
0x64
0x65
0x76

-- End predefined bytes to generate Rijndael Key and IV –

Relationship Summary

5d65ebdde1...	Related_To	d8d919d884b86e4d5977598bc9d637ed53e21d5964629d0427077e08ddbcba68
d8d919d884...	Related_To	5d65ebdde1aef8f23114f95454287e7410965288f144d880ece2a2b8c3128645

Recommendations

NCCIC would like to remind users and administrators to consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate ACLs.

Additional information on malware incident prevention and handling can be found in NIST's Special Publication 800-83, **Guide to Malware Incident Prevention & Handling for Desktops and Laptops.**

Contact Information

- 1-888-282-0870
- NCCICCustomerService@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

NCCIC continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://us-cert.gov/forms/feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the NCCIC at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to NCCIC? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov (anonymous)

NCCIC encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

Revisions

December 3, 2018: Initial version

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

GLESEC INFORMATION SHARING PROTOCOL

GLESEC CYBER SECURITY FLASH REPORTS are in compliance with the U.S. Department of Homeland Security (DHS) Traffic-Light Protocol (TLP): TLP-White (Disclosure is Not Limited), TLP-Green (Limited Disclosure, Restricted Only to the Community), TLP-Amber (Limited Disclosure, Restricted to the Participant's Organization), and TLP-Red (Not for Disclosure, Restricted/ Classified - Only Shared with US DHS).

Credits:

Homeland Security

US-CERT United States Computer Emergency Readiness Team