

Globelmposter 预警及勒索模块简单分析

信安之路应急响应小组

一、Globelmposter 简介

Globelmposter 家族首次出现在 2017 年 5 月份，2018 年 2 月全国各大医院受 Globelmposter 2.0 勒索病毒攻击，导致医院系统被加密，2018 年 12 月深信服 EDR 安全团队发现加密后缀为 '.fuck' 的 4.0 版本。

二、影响范围

2019 年 3 月，感染该勒索病毒事件进一步扩大，目标主要针对医疗机构，政府、企业、教育等行业均有波及。

三、行为分析

黑客通过入侵目标机构内网后，利用 RDP/SMB 暴力破解、CVE 漏洞利用等方法在内网环境传播 Globelmposter 勒索病毒，当然也不排除人工投毒的可能。

1) 加密后缀及版本划分

该勒索病毒在感染成功后，受害者主机上的文件将会被加密，文件名会加上后缀，不同版本加密后缀如下：

- ① Globelmposter 2.0 后缀：TECHNO、DOC、CHAK、FREEMAN、TRUE、ALC0、ALC02、ALC03、RESERVE 等；
- ② Globelmposter 3.0 变种后缀为以*4444 结尾，相对于 Globelmposter 2.0 版本，Globelmposter3.0 采用 RSA+AES 算法加密；
- ③ Globelmposter 4.0 为以 *.fuck 结尾。

2) 勒索模块分析

```
name: Dragon4444.exe
md5: C8F7EE073176EA98AF44F0FFC924815D
sha1: 60852D02BEBDBE1314AA8E6EB818DE2F316247DC
sha256: BD977050D237D581BAB7673844DA947472010371FDD6C28D2EAC6A1F55716043
```

size: 51712 bytes

cpu: 32-bit

加密模块样本链接: <https://github.com/Cherishao/APT-Sample>

样本关联 VirusTotal 情况如下, 被多家杀软识别为恶意文件。

c:\users\95190\desktop\glk	engine (63)	detection (47)	date (dd.mm.yyyy)	age (days)
	Endgame	malicious (high confidence)	15.02.2019	24
indicators (4/15)	Sophos	Troj/Ransom-EVE	28.02.2019	11
virustotal (47/63 - 23.02)	Comodo	Malware@#2lkxjvc166un	28.02.2019	11
dos-stub (!This program	DrWeb	Trojan.Encoder.26290	28.02.2019	11
file-header (Apr.2018)	Invincea	heuristic	28.11.2018	103
optional-header (GUI)	McAfee-GW-Edition	BehavesLike.Win32.Salitystub.qm	28.02.2019	11
directories (2)	Trapmine	malicious.high.ml.score	23.01.2019	47
sections (.rdata)	Emsisoft	Generic.Ransom.GlobelImposter.534A9...	28.02.2019	11
libraries (5)	SentinelOne	static engine - malicious	03.02.2019	36
imports (64/9/0/1/23)	Jiangmin	Trojan.Generic.cblhx	28.02.2019	11
exports (0)	Webroot	W32.Trojan.Gen	01.03.2019	10
tls-callbacks (n/a)	Avira	HEUR/AGEN.1011584	28.02.2019	11
resources (n/a)	Antiy-AVL	Trojan/Win32.Skeeyah	28.02.2019	11
strings (26/5/0/9/574)	Microsoft	Trojan:Win32/Skeeyah.Alrfrn	28.02.2019	11
debug (n/a)	ViRobot	Trojan.Win32.Ransom.75776.B	28.02.2019	11
manifest (n/a)	ZoneAlarm	HEUR:Trojan.Win32.Generic	28.02.2019	11
version (n/a)	GData	Generic.Ransom.GlobelImposter.534A9...	28.02.2019	11
certificate (n/a)	AhnLab-V3	Trojan/Win32.FileCoder.R228072	28.02.2019	11
overlay (n/a)	Acronis	suspicious	22.02.2019	17
	VBA32	BScope.TrojanRansom.Ergop	28.02.2019	11
	ALYac	Trojan.Ransom.GlobelImposter	28.02.2019	11
	MAX	malware (ai score=100)	01.03.2019	10
	Ad-Aware	Generic.Ransom.GlobelImposter.534A9...	28.02.2019	11
	Tencent	Win32.Trojan.Raas.Auto	01.03.2019	10
	Yandex	Trojan.Agent!BTxyThlMA/o	28.02.2019	11
	Ikarus	Trojan-Ransom.FileCrypter	28.02.2019	11
	Fortinet	W32/Filecoder.FVltr	28.02.2019	11
	AVG	Win32:Trojan-gen	28.02.2019	11
	Cybereason	malicious.73176e	09.01.2019	61
	Panda	Trj/Genetic.gen	28.02.2019	11
	CrowdStrike	win/malicious_confidence_100% (W)	12.02.2019	27
	Qihoo-360	Win32/Trojan.Necne.A	01.03.2019	10

勒索模块执行后, 主要有 2 个动作, 加密文件及修改注册表。

① 加密文件操作:加密文件及创建 名为 "How_TO_BACK_FILES.txt" 的 txt 文本。

进程详细信息

进程	任务组	线程	TCP/IP	
任务列表:				
进程ID	进程名	路径	公司名	描述
4908	Dragon4444.exe	C:\Users\95190\Desktop\globe...		
修改过的资源:				
修改操作	路径			
File Modify(128)				
touch modified	C:\ProgramData\VMware\VMware VgAuth\HOW_TO_BACK_FILES.txt			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\de\VGAuthCli.vmsg			
touch modified	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\en\HOW_TO_BACK_FILES.txt			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\en\VGAuthCli.vmsg			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\en\VGAuthLib.vmsg			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\en\VGAuthService.vmsg			
touch modified	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\es\HOW_TO_BACK_FILES.txt			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\es\VGAuthCli.vmsg			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\es\VGAuthLib.vmsg			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\es\VGAuthService.vmsg			
touch modified	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\fr\HOW_TO_BACK_FILES.txt			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\fr\VGAuthCli.vmsg			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\fr\VGAuthLib.vmsg			
modified remove	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\fr\VGAuthService.vmsg			
touch modified	C:\ProgramData\VMware\VMware VgAuth\msgCatalogs\messages\it\HOW_TO_BACK_FILES.txt			

加密方式，在 PE 文件中，可见：

	type	size	blacklist (26)	hint (5)	whitelist (0)	group (9)	import (0)	value (574)
indicators (4/15)	ascii	16	-	-	-	-	n/a	0123456789ABCDEF
virustotal (47/63 - 23.02)	ascii	6	-	-	-	-	n/a	SHA224
dos-stub (lThis program	ascii	6	-	-	-	-	n/a	SHA256
file-header (Apr.2018)	ascii	23	-	-	-	-	n/a	sha224WithRSAEncryption
optional-header (GUI)	ascii	16	-	-	-	-	n/a	RSA with SHA-224
directories (2)	ascii	23	-	-	-	-	n/a	sha256WithRSAEncryption
sections (.rdata)	ascii	16	-	-	-	-	n/a	RSA with SHA-256
libraries (5)	ascii	10	-	-	-	-	n/a	RSASSA-PSS
imports (64/9/0/1/23)	ascii	13	-	-	-	-	n/a	rsaEncryption
exports (0)	ascii	14	-	-	-	-	n/a	id-ecPublicKey
tls-callbacks (n/a)	ascii	14	-	-	-	-	n/a	Generic EC key
resources (n/a)	ascii	7	-	-	-	-	n/a	id-ecDH
strings (26/5/0/9/574)	ascii	15	-	-	-	-	n/a	EC key for ECDH
debug (n/a)	ascii	9	-	-	-	-	n/a	id-sha224
manifest (n/a)	ascii	7	-	-	-	-	n/a	SHA-224
version (n/a)	ascii	9	-	-	-	-	n/a	id-sha256
certificate (n/a)	ascii	7	-	-	-	-	n/a	SHA-256
overlay (n/a)								

② 修改注册表操作

Reg Modify(2)	
mkkey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
setval	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\BrowserUpdateCheck

四、处理方法

- ① 当发现网内某台主机感染 **Globelmposter** 勒索病毒后，立即断开受感染主机的网络（拔网线），因为病毒可能会通过 **SMB** 加密共享文件夹的文件，并利用一些攻击手法进行自我传播；
- ② 检查正在运行的进程，由于病毒程序会加载到内存空间运行，所以应先查看相关不明进程并结束相关病毒进程；
- ③ 利用杀毒软件或安全工具进行全盘杀毒，清除病毒及可疑程序，查杀完成后，尝试新建文件，确认文件不再会被加密；
- ④ 下载 **Globelmposter** 解密工具，参照使用指南尝试进行文件解密,解密工具检索站点如下：
<https://www.nomoreransom.org/zh/decryption-tools.html>
经测试，该解密工具对 **Globelmposter 3.0** 加密的文件，无法修复。
- ⑤ 最后，对局域网内的所有主机进行详细的安全检查和加固，确保网内主机的洁净与安全。

五、安全建议

- ① 不要点击来源不明的邮件附件，不从不明网站下载软件；
- ② 在主机上安装安全软件，保证主机免受已知的病毒侵袭；
- ③ 及时给主机打补丁(永恒之蓝漏洞补丁)，修复相应的高危漏洞；
- ④ 更改默认 **administrator** 管理帐户，禁用 **445** 等高危端口；
- ⑤ **RDP** 远程服务器等连接尽量使用强密码，字母大小写，数字及符号组合的密码，不低于 **10** 位字符；
- ⑥ 外网主机不应具备访问及修改内网主机数据的权限；
- ⑦ 设置帐户锁定策略，在输入 **5** 次密码错误后禁止登录；
- ⑧ 定期对重要文件进行异地备份，如果是云服务器，则必须做好快照。

六、参考链接

<http://url.cn/5SRjECE>

<https://www.freebuf.com/articles/terminal/193895.html>