

威胁情报 | APT41组织最新Winnti ELF后门

 ctfiot.com/304410.html



威胁简报

恶意软件

漏洞攻击

一、样本概况

安全研究员TuringAlex (@TuringAlex, Xlab_qax团队) 近日在公开平台披露了一个全新的Winnti ELF后门样本。该样本SHA256哈希为：f1403192ad7a762c235d670e13b703c3

关键特征如下：

- VirusTotal零检测：截至披露时，主流杀毒引擎均未检出。
- VMProtect全保护：样本采用VMProtect虚拟化加壳，极大提升了逆向分析难度。
- ELF格式：针对Linux环境设计，属于Winnti家族的跨平台变体。

这枚样本的出现，标志着Winnti组织继续深化对Linux服务器的渗透能力，尤其在绕过传统检测机制方面表现出色。

二、技术细节

通过对样本的二进制结构分析，我们发现以下显著特征：

1.自定义ELF节区

该ELF文件包含两个非标准节区：.eDM0 和 .eDM1。这些节区被标记为PROG XA类型，与已知Winnti家族样本的特征高度吻合，是识别该组织新型变体的重要指纹。

[X]

??	Num	Name	Type	Flg	VirtAddr	Offset	????????
?	13	.rodata	PROG	.A.	00000000`00408148	00000000`00008148	?
?	14	.eh_frame_hdr	PROG	.A.	00000000`00E9CC60	00000000`0029CC60	?
?	15	.eh_frame	PROG	.A.	00000000`00E9CE84	00000000`0029CE84	?
?	16	.ctors	PROG	.AW	00000000`0060A000	00000000`00000290	?
?	17	.dtors	PROG	.AW	00000000`0060A010	00000000`000002A0	?
?	18	.jcr	PROG	.AW	00000000`0060A020	00000000`000002B0	?
?	19	.dynamic	DYN	.AW	00000000`00E9D7F8	00000000`0029D7F8	?
?	20	.got	PROG	.AW	00000000`0060A1C8	00000000`00000458	?
?	21	.got.plt	PROG	.AW	00000000`00A7D640	00000000`0007D640	?
?	22	.data	PROG	.AW	00000000`0060A4C0	00000000`00000750	?
?	23	.bss	BSS	.AW	00000000`0060A8A0	00000000`00000B30	?
?	24	.shstrtab	STR	...	00000000`00000000	00000000`0029D968	?
?	25	.eDM0	PROG	XA.	00000000`0080A8A0	00000000`0000A8A0	?
?	26	.eDM1	PROG	XA.	00000000`00A00290	00000000`00000290	?
??	Offset out ???						

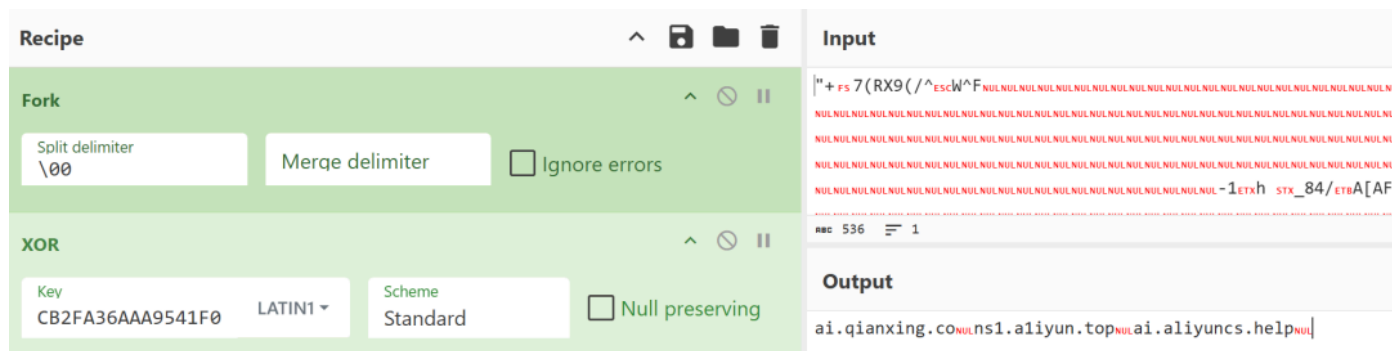
0000000	22	2B	1C	37	28	52	58	39	28	2F	5E	1B	57	5E	46	00	"+.7(RX9(/^.W^F.
0000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000100	2D	31	03	68	20	02	5F	38	34	2F	17	41	5B	41	46	00	-1.h.._84/.A[AF.
0000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000200	22	2B	1C	27	2D	5A	4F	34	2F	22	4A	1B	5C	54	2A	40	"+. '-Z04/"J.\T*@
0000210	43	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	C.....

2.C2域名加密机制

研究人员使用CyberChef工具，以16进制密钥 CB2FA36AAA9541F0（Latin1编码）进行XOR解密操作，成功还原出多个C2域名：

- ai.qianxing.co
- ns1.aliyun.top
- ai.aliyuncs.help

值得注意的是，其中ai.qianxing.co明显模仿了某安全研究团队的域名结构，显示出威胁行为体在针对性情报收集和伪装上的精心设计。



这些C2域名目前已成为重要的IOC（威胁情报指标），建议各单位立即纳入监控清单。

三、组织背景与趋势判断

APT41组织（又称Winnti组织）长期以开发高隐蔽性、跨平台后门闻名。该组织在Windows平台积累了丰富的经验后，近年来显著加强了对Linux、macOS等非Windows环境的适配。此次ELF变体的快速迭代，再次验证了其在持久化威胁与反检测技术上的持续投入。

从威胁情报角度看，此类样本通常服务于长期潜伏、数据窃取等目的。VMProtect+自定义节区+XOR加密的组合，体现了当前高级威胁行为体在“低慢小”攻击模式下的典型演进路径。

附IOC（供参考）：

SHA256: f1403192ad7a762c235d670e13b703c3

C2:

ai.qianxing.co

ns1.aliyun.top

ai.aliyuncs.help

XOR密钥:CB2FA36AAA9541F0

END



公众号内容都来自国外平台-所有文章可通过点击阅读原文到达原文地址或参考地址

排版 编辑 | Ots 小安

采集 翻译 | Ots Ai牛马

公众号 | AnQuan7 (Ots安全)

| 本篇文章来源于微信公众号: Ots安全