BOLETIM DE SEGURANÇA

Nova variante Linux do Ransomware Play mirando em sistemas VMware ESXi

heimdall
security research
A DIVISION OF ISH

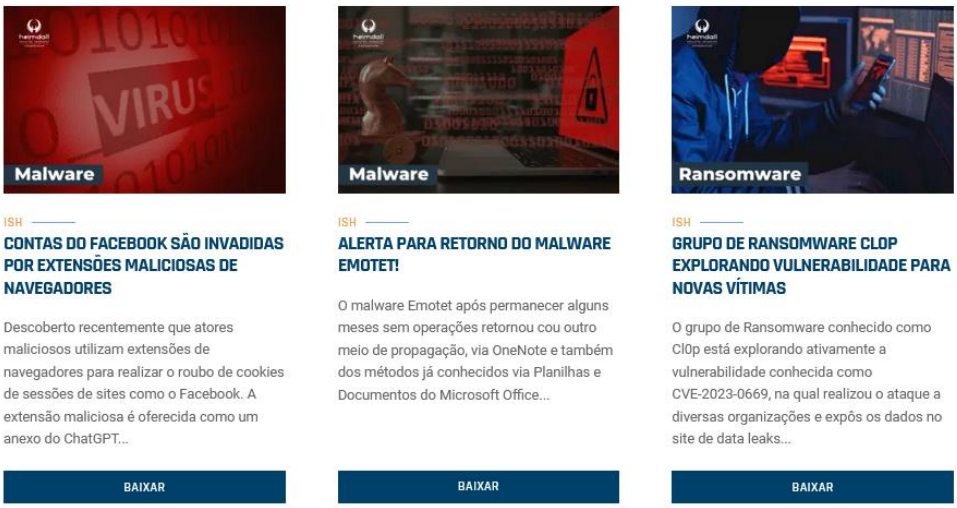
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Uma nova variante do ransomware Play, também conhecido como Balloonfly e PlayCrypt, foi identificada por pesquisadores de segurança cibernética. Esta variante, que opera no sistema operacional Linux, foi projetada especificamente para atacar ambientes VMware ESXi.

2 INFORMAÇÕES SOBRE A AMEAÇA

A equipe da Trendmicro, descobriu uma nova variante do ransomware Play que opera no Linux e criptografa arquivos apenas quando é executado em um ambiente VMware ESXi. O ransomware Play, que foi detectado pela primeira vez em junho de 2022, ganhou notoriedade por suas táticas de extorsão dupla, técnicas de evasão, ferramentas personalizadas e impacto significativo em várias organizações na América Latina. Esta é a primeira vez que o ransomware Play é observado visando ambientes ESXi. Este desenvolvimento sugere que o grupo pode estar expandindo seus ataques para a plataforma Linux, o que pode resultar em um maior número de vítimas e negociações de resgate mais bem-sucedidas.

Os ambientes VMware ESXi são comumente utilizados por empresas para executar várias máquinas virtuais (VMs). Eles geralmente hospedam aplicativos e dados críticos e normalmente incluem soluções de backup integradas. Comprometer esses ambientes pode interromper significativamente as operações comerciais e até mesmo criptografar backups, reduzindo ainda mais a capacidade da vítima de recuperar dados.

Figura 1 – Porcentagem de vítimas por países.

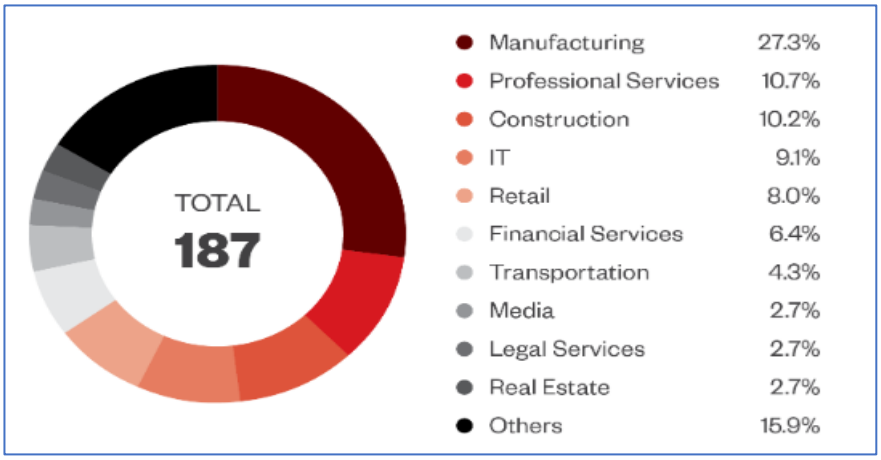


Figura 2 – Porcentagem de vítimas por setor.

A amostra enviada ao VirusTotal indica que ela conseguiu evitar detecções de segurança. Na análise, descobriu-se que a variante Linux está compactada em um arquivo RAR junto com sua variante Windows e está hospedada na URL, hxxp://108.[BLOCKED].190/FX300.rar.

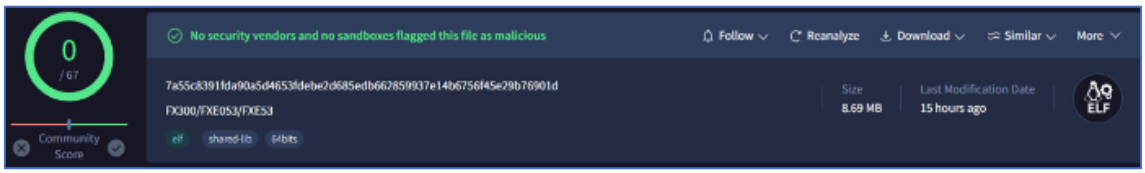


Figura 3 – Variante Linux do ransomware Play.

Este endereço IP contém ferramentas que foram usadas pelo ransomware Play em seus ataques anteriores, incluindo PsExec, NetScan, WinSCP, WinRAR e o backdoor Coroxy. Embora nenhuma infecção real tenha sido observada, o servidor de comando e controle (C&C) hospeda as ferramentas comuns que o ransomware Play usa atualmente em seus ataques. Isso pode indicar que a variante Linux pode empregar táticas, técnicas e procedimentos (TTPs) semelhantes.

Assim como sua variante para Windows, o exemplo aceita argumentos de linha de comando, mas seus comportamentos ainda são desconhecidos.

Jogue Ransomware Variante do Windows	Descrição	Jogue Ransomware Variante Linux	Descrição
-mc	Executar funcionalidade normal; o mesmo que nenhum argumento de linha de comando	-p	N / D
-d <caminho da unidade>	Criptografar uma unidade específica	-f	N / D
-ip <caminho do recurso compartilhado> <nome de usuário> <senha>	Criptografar recurso compartilhado de rede	-s	N / D
-p <caminho>	Criptografar uma pasta/arquivo específico	-e	N / D

Figura 4 – inha de comando das variantes Windows e Linux do ransomware Play.

O exemplo executa comandos relacionados ao ESXi para verificar se está sendo executado em um ambiente ESXi antes de executar suas rotinas maliciosas. Caso contrário, ele será encerrado e excluído. Também foi encontrado uma série de comandos de script de shell que o exemplo executa quando está em execução em um ambiente ESXi. O comando abaixo é responsável por escanear e desligar todas as VMs encontradas no ambiente:

```
/bin/sh -c "for vmid in $(vim-cmd vmsvc/getallvms | grep -v Vmid | awk '{print $1}');
do vim-cmd vmsvc/power.off $vmid; done"
```

Figura 5 – Comando abaixo é responsável por escanear e desligar todas as VMs encontradas.

Depois que o ransomware executa a série de comandos relacionados ao ESXi, ele prossegue para criptografar arquivos de VM, incluindo disco de VM, configuração e arquivos de metadados. O arquivo de disco de VM, por exemplo, contém dados críticos, incluindo aplicativos e dados do usuário.

```
aVmdk           db '.vmdk',0
aVmem           db '.vmem',0
aVmsd           db '.vmsd',0
aVmsn           db '.vmsn',0
aVmx            db '.vmx',0
aVmxf           db '.vmxf',0
aVswp           db '.vswp',0
aVmss           db '.vmss',0
aNvram          db '.nvram',0
aVmtx           db '.vmtx',0
aLog            db '.log',0
```

Figura 6 – Lista de extensões a serem criptografadas.

Monitorando as atividades externas do endereço IP suspeito, observou-se que a URL usada para hospedar a carga do ransomware e suas ferramentas está relacionada a outro agente de ameaça, chamado Prolific Puma. Esse agente é conhecido por gerar nomes de domínio usando um algoritmo gerador de destino aleatório (RDGA) e os utiliza para oferecer um serviço de encurtamento de links para outros criminosos cibernéticos, que o usam para evitar a detecção enquanto disseminam esquemas de phishing, golpes e malware.

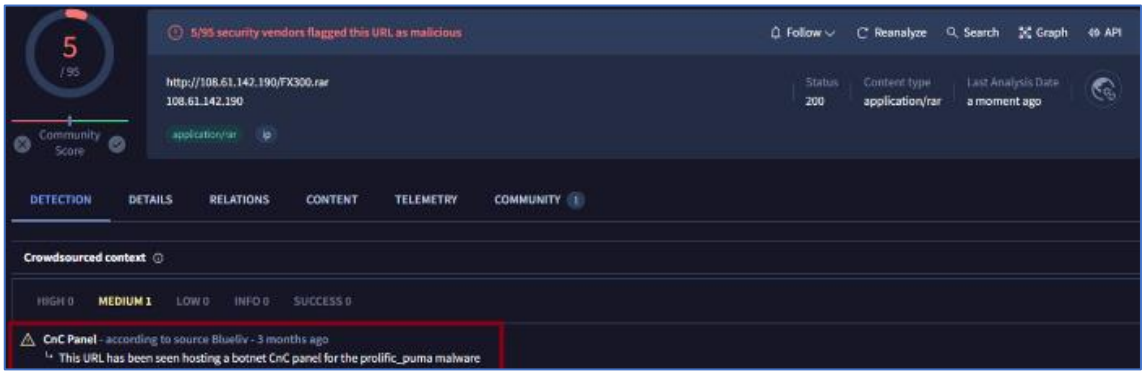


Figura 7 – Resultado do VirusTotal da URL menciona Prolific Puma.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Defense Evasion	T1070.004	Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento.
Discovery	T1046 T1083	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Execution	T1059.004	Consiste em técnicas que resultam em código controlado pelo adversário em execução em um sistema local ou remoto.
Lateral Movement	T1570	Consiste em técnicas que os adversários usam para entrar e controlar sistemas remotos em uma rede.
Command and Control	T1568.002 T1105	Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima.
Exfiltration	T1041	Consiste em técnicas que adversários podem usar para roubar dados da sua rede. Depois de coletar dados, os adversários geralmente os empacotam para evitar a detecção ao removê-los.
Impact	T1486 T1491.001 T1489	Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade ao manipular processos comerciais e operacionais.

Tabela 1 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Aplicação de patches e atualizações regulares

- Mantenha o ambiente ESXi e o software de gerenciamento associado atualizados para proteger contra vulnerabilidades conhecidas.

Patching virtual

- Muitas organizações podem não aplicar patches ou atualizar seus ambientes ESXi com a frequência que deveriam devido à complexidade, preocupações com tempo de inatividade, restrições de recursos, prioridades operacionais ou problemas de compatibilidade.

Abordando configurações incorretas inerentes

- Audite e corrija regularmente configurações incorretas em ambientes ESXi, pois elas podem criar vulnerabilidades que o ransomware pode explorar.

Controles de acesso rigorosos

- Implemente mecanismos robustos de autenticação e autorização, como autenticação multifator (MFA), e restrinja o acesso administrativo.

Segmentação de rede

- Separe sistemas e redes críticas para limitar a disseminação de ransomware.

Superfície de ataque minimizada

- Desabilite serviços e protocolos desnecessários e não utilizados, restrinja o acesso a interfaces de gerenciamento críticas e implemente regras de firewall rígidas para limitar a exposição da rede.

Backups offline regulares

- Mantenha backups frequentes e seguros de todos os dados críticos. Garanta que os backups sejam armazenados offline e testados regularmente para verificar sua integridade.

Monitoramento de segurança e resposta a incidentes

- Implante soluções e desenvolva um plano de resposta a incidentes para abordar atividades suspeitas de forma rápida e proativa.

5 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	1fa3574bb8f45497dbbf8421d0444428
sha1:	2a5e003764180eb3531443946d2f3c80ffcb2c30
sha256:	7a55c8391fda90a5d4653fdebe2d685edb662859937e14b6756f45e29b76901d
File name:	2024-05-30_1fa3574bb8f45497dbbf8421d0444428_revil

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxp://108.61.142[.]190/FX300.rar hxxp://108.61.142[.]190/1.dll.sa hxxp://108.61.142[.]190/64.zip hxxp://108.61.142[.]190/winrar-x64-611.exe hxxp://108.61.142[.]190/PsExec.exe hxxp://108.61.142[.]190/host1.sa
IP	108.61.142[.]190

Tabela 3 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **TrendMicro**
- **Thehackernews**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH