heimdall

security research

A DIVISION OF ISH

Junho 2022

RELATÓRIO SEMESTRAL

JUN 2022

heimdall
security research

APRESENTAÇÃO

Sem dúvidas, ataques de *ransomware* constituíram o maior desafio da área de segurança cibernética até o momento em 2022.
Enquanto alguns grupos maliciosos que operam como redes de *ransomware-as-a-service* (RaaS) afirmam evitar ataques a hospitais ou outros setores críticos que podem causar danos às pessoas, grupos como Hive atacam setores de saúde, não tendo consideração pela vida humana. Somado a esta adversidade estão as vulnerabilidades, a configuração de sistemas (*misconfiguration*), a necessidade de otimização de processos e o constante desafio em obter informações claras sobre estas ameaças.

O Heimdall, grupo de Threat Intelligence da ISH Tecnologia, apresenta neste material as informações mais relevantes sobre estes grandes desafios, revelando ferramentas utilizadas por grupos maliciosos, Indicadores de Comprometimento, Técnicas, Táticas e Procedimentos (TTPs) entre outros.

Estamos certos de que este material lhe atenderá como um guia em sua missão de ampliar a inteligência de ameaças de sua empresa!

Paulo Trindade - Manager | Information Security Officer

RELATÓRIO SEMESTRAL

JUN 2022

12 AMEAÇAS RECORRENTES

08 GRUPOS DE RANSOMWARE

03 TTPS INITIAL ACCESS

TOP #06 - VULNERABILIDADES E EXPLOITS

#1	EXPLOIT.SCRIPT.CVE-2021-26855.E
#2	EXPLOIT.SCRIPT.GENERIC
#3	EXPLOIT.MSOFFICE.CVE-2018-0802.GEN
#4	EXPLOIT.HTTP.CVE-2017-5638.GEN
#5	EXPLOIT.MSOFFICE.CVE-2017-11882.GEN
#6	EXPLOIT.WIN32.CERTUTIL.GE

TOP #06 - RANSOMWARES

#1	TROJAN-RANSOM.WIN32.WANNA.ZBU
#2	TROJAN-RANSOM.MSIL.BLOCKER.GEN
#3	TROJAN-RANSOM.WIN32.CONVAGENT.GEN
#4	TROJAN-RANSOM.WIN32.PHNY.A
#5	TROJAN-RANSOM.WIN32.STOP.GEN
#6	TROJAN-RANSOM.WIN32.WANNA.M

TOP #08 - GRUPOS DE RANSOMWARE

#1	CONTI/RYUK	#484	53,1%
#2	PYSA	#149	16,4%
#3	CLOP (TA505)	#114	12,5%
#4	HIVE	#50	5,5%
#5	LOCKBIT2.0	#31	3,4%
#6	RAGNARLOCKER	#28	3,1%
#7	BLACKCAT	#28	3,1%
#8	BLACKBYTE	#27	3%

911 VÍTIMAS IDENTIFICADAS

TOP #03 - TTPS INITIAL ACCESS

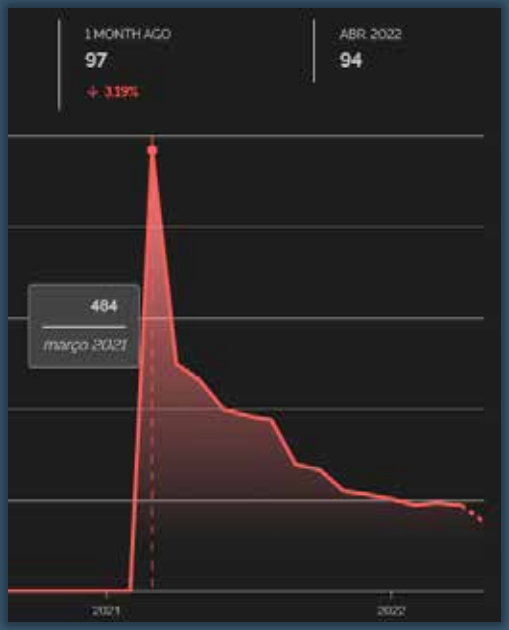
#1	T1133	EXTERNAL REMOTE SERVICES
#2	T1190	EXPLOIT PUBLIC-FACING APPLICATION
#3	T1566	PHISHING

TOP #08 - GRUPOS DE RANSOMWARE

1 TOP 06 VULNERABILIDADES E *EXPLOITS*

1# Exploit.Script.CVE-2021-26855.e

Essa família consiste em arquivos maliciosos que exploram a vulnerabilidade de falsificação de solicitação do lado do servidor (SSRF) CVE-2021-26855. Esses arquivos permitem enviar solicitações HTTP arbitrárias e autenticar-se como Microsoft Exchange Server.



Apesar de ser uma vulnerabilidade de março de 2021, no Brasil, ainda pode-se encontrar **quase 100** servidores vulneráveis.

Em pesquisa global, cerca de **6.858** *hosts* estão vulneráveis e suscetíveis a um ataque.

#2 Exploit.Script.Generic

Aplicativos dessa família são *scripts* mal-intencionados que tentam explorar as vulnerabilidades do ***software* do sistema**.

#3 Exploit.MSOffice.CVE-2018-0802.gen

Essa família consiste em um *malware* que explora a vulnerabilidade CVE-2018-0802. Existe uma vulnerabilidade de execução remota de código no **Microsoft Office** quando o *software* não consegue manipular corretamente os objetos na memória. Um invasor que explora com êxito esta vulnerabilidade pode executar **código arbitrário** no contexto do usuário atual. Se ele estiver conectado com direitos de usuário administrativo, um invasor poderá assumir o **controle do sistema afetado**.

#4 Exploit.HTTP.CVE-2017-5638.gen

O *parser* do Jakarta Multipart do Apache Struts 2 versões 2.3.X até 2.3.32 e Apache Struts 2 versões 2.5.X até 2.5.10.1 gerencia incorretamente o tratamento de exceções e a geração de mensagens de erro durante as tentativas de upload de arquivos, o que permite que invasores executem remotamente comandos arbitrários por meio de cabeçalhos HTTP Content-Type, Content-Disposition ou Content-Length criados propositadamente.

#5 Exploit.MSOffice.CVE-2017-11882.gen

O *malware* desta família explora uma vulnerabilidade do Microsoft Equation Editor (geralmente incluído no Microsoft Office). Se um ataque for bem-sucedido, o invasor ganha a capacidade de executar algum código na conta de um usuário.

#6 Exploit.Win32.Certutil.ge

O Windows possui um programa interno chamado CertUtil que pode ser usado para gerenciar certificados no Windows. Usando este programa, pode-se instalar, fazer *backup*, excluir, gerenciar e executar várias funções relacionadas a certificados e armazenamentos de certificados no Windows.

Tal *exploit* abusa de um dos recursos do CertUtil, que é a capacidade de baixar um certificado, ou qualquer outro arquivo, de uma URL remota e salvá-lo como um arquivo local.

2 *RANSOMWARES*

#1 Trojan-Ransom.Win32.Wanna.zbu

Consiste em um *malware* do tipo WannaCry. Este criptografa arquivos do usuário e costuma ser distribuído explorando uma vulnerabilidade do protocolo SMB.

#2 Trojan-Ransom.MSIL.Blocker.gen

Depois que o trojan é instalado em um computador, ele se adiciona à rotina de inicialização e bloqueia o carregamento normal do sistema operacional. Quando o sistema operacional é iniciado, o trojan assume o controle do computador e exibe uma janela solicitando que o usuário envie uma mensagem SMS com texto especial para o número indicado. Em troca, a janela indica que o usuário receberá um código para desativar o *malware* e desbloquear o acesso ao computador.

#3 Trojan-Ransom.Win32.Convagent.gen

Este *ransomware* normalmente chega em um sistema como um arquivo descartado por outro *malware* ou como um arquivo baixado pelos usuários sem que eles soubessem ao visitar *sites* maliciosos e descarta arquivos como nota de resgate.

#4 Trojan-Ransom.WIN32.Phny.a

Parte da família do WannaCry, responsável por 32,40% das detecções no último mês no Brasil e 8,83% no mundo.

#5 Trojan-Ransom.Win32.Stop.gen

Geralmente é proveniente de um *malware* que foi baixado no sistema da vítima ou através do *download* de arquivos na internet sem o conhecimento dos usuários ao visitar *sites* maliciosos.

#6 Trojan-Ransom.Win32.Wanna.m

Assim como o #1 Wanna.zbu, esse trojan consiste em um *malware* do tipo WannaCry.

3 GRUPOS DE *RANSOMWARE*

#1 Conti / Ryuk

Considerado o sucessor do *ransomware* Ryuk, Conti é atualmente uma das famílias de *ransomware as a service* mais ativas e conhecidas.

Seus operadores utilizam técnicas de dupla extorsão – *double extortion* e, além da publicação de dados roubados, também colocam à venda acessos às organizações de vítimas que se recusaram a pagar o resgate.

#2 PYSA

PYSA é considerada uma variante do *ransomware* Mespinoza.

PYSA, que significa *Protect Your System Amigo* - Proteja Seu Sistema Amigo, também é categorizada como um RaaS - *Ransomware as a Service*.

#3 Clop (TA505)

Clop também conhecido como "Cl0p", evoluiu como uma variante da família de *ransomware* CryptoMix e ganhou fama por comprometer organizações de alto perfil em vários setores em todo o mundo.

#4 Hive

O Hive se tornou uma das famílias de *ransomware* mais ativas desde sua descoberta em junho de 2021 e é conhecido por ter novas ferramentas de *malware* desenvolvidas especificamente para criptografar sistemas Linux e FreeBSD.

#5 Lockbit2.0

O LockBit 2.0 é um *ransomware* como serviço (RaaS) que surgiu pela primeira vez em junho de 2021 e, desde a sua criação, vem atraindo afiliados por meio de campanhas de recrutamento em fóruns *undergrounds*.

Seus operadores afirmaram ter o *software* de criptografia mais rápido de qualquer linhagem de *ransomware* ativa em junho 2021.

#6 RagnarLocker

Descoberto inicialmente em abril de 2020, o Ragnar Locker é conhecido por mudar constantemente suas técnicas de ofuscação para evitar detecção e prevenção, além de impedir que as organizações entrem em contato com as autoridades após uma violação.

#7 BlackByte

O BlackByte foi visto pela primeira vez em julho de 2021. Os operadores exploraram as vulnerabilidades do *ProxyShell* para se firmar no ambiente da vítima. Ele tem semelhanças com outras variantes de *ransomware*, como o Lockbit 2.0, que evitam sistemas que usam russo e vários idiomas do leste europeu.

#8 BlackCat

BlackCat (também conhecido como AlphaVM ou AlphaV) é uma família de *ransomware* criada na linguagem Rust e possui versões que funcionam nos sistemas operacionais Windows e Linux, bem como ESXi da VMware.

Neste mês, o grupo começou a publicar *sites* na internet com o nome da vítima no domínio e seu logo na página inicial, contendo os dados vazados disponibilizados em um formulário facilmente pesquisável.

4 TTPs - *INITIAL ACCESS*

Entre os grupos mais comuns de *ransomware* atribuídos aos ataques atuais, existem essencialmente três maneiras pelas quais o acesso inicial é obtido:

1. Explorando serviços publicamente disponíveis (por exemplo, um servidor HTTP ou um servidor VPN);
2. Aplicando técnicas de *(spear)phishing*;
3. Compra de acesso, podendo ser de:
    a. Credenciais.
    b. Dispositivo infectado com um *malware* dentro da organização.

***External Remote Services* – MITRE ATT&CK ID: T1133**

Os atores de ameaças podem tirar proveito de serviços remotos externos para conseguir acesso inicial à rede e/ou até mesmo persistência nela. Serviços remotos permitem que os usuários se conectem a recursos internos de uma rede corporativa a partir de locais externos, como por exemplo, *Windows Remote Management*, VNC e RDP.

Ter acesso a contas válidas para usar tais serviço geralmente é um requisito que pode ser obtido por meio de *pharming* [1] de credenciais e/ou compra do acesso.

O acesso inicial também pode ser obtido por meio de um serviço exposto que não requer autenticação, como em ambientes em contêiner, podendo incluir uma API do Docker exposta, servidor de API do Kubernetes, kubelet ou aplicativo da *Web*, como o painel do Kubernetes.

***Exploit Public-Facing Application* – MITRE ATT&CK ID: T1190**

Os adversários podem se utilizar de uma vulnerabilidade em um sistema voltado para a internet usando *software*, dados ou comandos para causar um comportamento não intencional ou imprevisto. O ponto de acesso ao sistema pode ser um *bug*, uma falha ou uma vulnerabilidade de design. Esses aplicativos geralmente são *sites*, mas podem incluir bancos de dados, serviços padrão (como SMB ou SSH), protocolos de administração e gerenciamento de dispositivos de rede (como SNMP e Smart Install) e quaisquer outros aplicativos com *sockets* abertos acessíveis à internet.

***Phishing* – MITRE ATT&CK ID: T1566**

Atacantes enviam mensagens de *phishing* para obter acesso aos sistemas das vítimas por meio de engenharia social. O *phishing* pode ser direcionado – conhecido como *spearphishing*, no qual um indivíduo, empresa ou setor específico será o alvo do adversário –, ou *phishing* não direcionado que, de maneira mais geral, é executado em campanhas de *spam* de *malware* em massa.

Tais e-mails normalmente contêm anexos ou *links* maliciosos, normalmente para executar código malicioso nos sistemas das vítimas; porém, também pode ser realizado por meio de serviços de terceiros, como plataformas de mídia social.

[1] *Pharming*, uma junção das palavras "*phishing*" e "*farming*", é um ataque online semelhante ao *phishing*, onde o tráfego de um *site* é manipulado e informações confidenciais são roubadas.

5 VULNERABILIDADES E SERVIÇOS MAIS EXPLORADOS

O serviço mais atacado é o **RDP**, no qual são tentadas combinações de nome de usuário/senha fracos para se obter acesso, sendo como um ponto de apoio dentro da organização alvo. Credenciais vazadas e compradas também são uma alternativa.

Já com relação a vulnerabilidades de aplicativos, as mais comumente exploradas são:

ProxyShell CVEs	Vulnerabilidades no Microsoft Exchange que podem permitir que um invasor remoto execute código arbitrário em um Servidor.
CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	

Com o *phishing*, e-mails contendo documentos do Office que enganam a vítima para habilitar macros são os mais populares e, como consequência, a execução da sub-técnica **T1204.002** - User Execution: Malicious File. Adicionalmente, os adversários podem usar vários outros tipos de arquivos que exigem que um usuário os execute, incluindo .pdf, .scr, .exe, .lnk, .pif e .cpl.

Embora o arquivo malicioso mencionado seja enviado para o acesso inicial, ele pode ocorrer em outras fases de uma invasão, como quando um invasor coloca um arquivo em um diretório compartilhado ou na área de trabalho de um usuário esperando que ele clique nele.

6 FERRAMENTAS MAIS UTILIZADAS

Analisando os grupos listados por serem mais comuns nos ataques atuais, foi possível criar uma lista de utilitários conhecidos usados por esses operadores de *ransomware*:

Atores de ameaça	Ferramentas
Hive	PsExec, RedLine Stealer, CobaltStrike, NBMiner, dxdiag, Advanced IP Scanner, PCHunter, GMER, Bloodhound
Clop	FlawedAmmyy RAT, CobaltStrike, TinyMet, SDBOT, DEWMODE, Get2 Loader
Lockbit	Mimikatz, PsExec, Koadic, Empire, LaZagne
RagnarLocker	CobaltStrike
Conti	QBot, IcedID, CobaltStrike
Pysa	Gasket, PsExec
Blackbyte	CobaltStrike, Mimikatz, AnyDesk, SoftPerfect Network Scanner, Process Explorer, PowerView
BlackCat	PsExec, CobaltStrike, Mimikatz, WebBrowserPassView, Koadic, Empire, LaZagne

7 IoCs

Como forma de auxiliar na rápida detecção de ameaças, selecionamos os indicadores mais recorrentes em ataques no Brasil durante o último mês. Entre eles estão ***hashes* MD5, URLs e C&C – Comando e Controle**.

Tais indicadores ajudam na detecção de violações de dados, infecções por *malware* ou outras atividades maliciosas. Ao monitorar os indicadores de comprometimento, pode-se detectar ataques e agir rapidamente para evitar que ocorram violações ou limitar os danos interrompendo os ataques em estágios iniciais.

Top 10 C&C	Top 10 URLs	Top 10 MD5
vencedoresverdadeiros.cloud	vencedoresverdadeiros.cloud	F59A68D0FBA45DBD5F927E447F0B3C45
iustinus-agi.com	donttbeevils.de	B031E991F354D7FA51E7682452B3D5C1
organizadoorgulhoso.one	wp20.ru	41920D440AC656C1230FC9EB5D98ABD2
mwenautica.com	rtbxheartbid.com	A92AC7258F65552C7B77D27CCE4E1E01
adsperfection.go2affise.com	ugroocuw.net	C5AA9FF98FDBE81503F1EE1318C0D674
modesta-gor.com	xtfycjyzoqit.com	D7192C29E831E744738E5D96362EA9D4
intensointeressante.cloud	104.155.207.188	A96362B2CE68A64777AD8786A0265CD3
apiujquery.com	parkistanmebbelonline.com	D531F76F87685065A11711946A2C4039
nevagandosegurof.sbs	f1leloadinf.com	E28C4F9CC07E97CDF07D0127FCEFF603
loucolouvavel.us	exceptcontrolreach.xyz	B1971537931AE9BBF846893F9E3C3785

vencedoresverdadeiros[.]cloud

Categoria: Botnet C&C (Trojan.WinLNK.Agent), *Malware*

Detecções: Mais de 6 mil

F59A68D0FBA45DBD5F927E447F0B3C45

Categoria: *Malware*

Detecções: Mais de 20 mil

Arquivo acessa a seguinte URL:

http[.]vidadigitalcelular[.]com

8 CONCLUSÃO

Diante do cenário exposto, percebe-se que o Brasil ainda precisa melhorar a sua postura digital. Várias novas ameaças surgem todos os dias, cada vez mais resilientes e complexas, exigindo das organizações mais atenção e cuidado com os seus ativos, investimento em treinamentos para seus usuários e constante atualização.

Os dados informados neste boletim ajudam na mitigação e prevenção das ameaças em destaque no momento e as recomendações a seguir são um complemento importante no combate a possíveis ataques.

9 RECOMENDAÇÕES

1. **Mantenha *backups* de dados criptografados e *offline* e teste-os com frequência**. Os procedimentos de *backup* devem ser realizados regularmente. É importante que os *backups* sejam mantidos *offline*, pois muitas variantes do *ransomware* tentam localizar e excluir ou criptografar *backups* acessíveis.

2. **Crie, mantenha e execute um plano básico de resposta a incidentes cibernéticos, um plano de recuperação e um plano de comunicações associado.**

- O plano de resposta a incidentes cibernéticos deve incluir procedimentos de resposta e notificação para incidentes de *ransomware*. Recomendamos o *CISA and Multi-State Information and Sharing Center (MS-ISAC) Joint Ransomware Guide* para obter mais detalhes sobre a criação de um plano de resposta a incidentes cibernéticos.
- O plano de recuperação deve abordar como operar se você perder o acesso ou o controle de funções críticas. A CISA oferece avaliações de resiliência cibernética sem custo e não técnicas para ajudar as organizações a avaliar sua resiliência operacional e práticas de segurança cibernética.

3. **Mitigar vulnerabilidades e configurações incorretas voltadas para a Internet para reduzir o risco de atores que exploram essa superfície de ataque:**

a. Empregue as melhores práticas para o uso de *Remote Desktop Protocol* (RDP) e outros serviços de área de trabalho remota. Os atores da ameaça geralmente obtêm acesso inicial a uma rede por meio de serviços remotos expostos e mal protegidos e, posteriormente, propagam o *ransomware*.

Audite a rede para sistemas usando RDP, portas RDP fechadas não usadas, aplique bloqueios de conta após um número especificado de tentativas, aplique autenticação multifator (MFA) e registre tentativas de *login* RDP.

b. Realize varreduras de vulnerabilidades regulares para identificar e resolver vulnerabilidades, especialmente aquelas em dispositivos voltados para a Internet. A CISA oferece uma variedade de serviços de higiene cibernética gratuitos, incluindo varredura de vulnerabilidade, para ajudar as organizações de infraestrutura crítica a avaliar, identificar e reduzir sua exposição a ameaças cibernéticas, como *ransomware*. Tirando proveito desses serviços, as organizações de qualquer porte receberão recomendações sobre maneiras de reduzir seus riscos e mitigar vetores de ataque.

c. Atualize o *software*, incluindo sistemas operacionais, aplicativos e *firmware*, em tempo hábil. Priorize a correção oportuna de vulnerabilidades críticas e vulnerabilidades em servidores voltados para a Internet – bem como *software* de processamento de dados da Internet, como navegadores da *web*, *plug-ins* de navegador e leitores de documentos. Se a correção rápida não for viável, implemente as atenuações fornecidas pelo fornecedor.

d. Certifique-se de que os dispositivos estejam configurados corretamente e os recursos de segurança estão ativados; por exemplo, desativar portas e protocolos que não estão sendo usados para uma finalidade comercial.

e. Desative ou bloqueie o protocolo SMB (*Server Message Block*) de entrada e saída e remova ou desative as versões desatualizadas do SMB.

4. **Reduza o risco de e-mails de *phishing* chegarem aos usuários finais:**

a. Habilitando filtros de *spam*.

b. Implementando um programa de conscientização e treinamento do usuário de segurança cibernética que inclua orientação sobre como identificar e relatar atividades suspeitas (por exemplo, *phishing*) ou incidentes.

5. **Utilize as melhores práticas disponíveis de segurança cibernética:**

a. Garanta que todos os *softwares* antivírus, *antimalwares* e assinaturas estejam atualizados.

b. Implemente a lista de permissões de aplicativos (*application allowlisting*).

c. Garanta que as contas de usuários e privilégios sejam limitadas por meio de políticas de uso de contas, controle de contas de usuários e gerenciamento de contas com privilégios.

d. Empregue MFA para todos os serviços que forem possíveis, especialmente para *webmail*, redes privadas virtuais (VPNs) e contas que acessam sistemas críticos.

10 REFERÊNCIAS

1. Kaspersky
2. welivesecurity.com
3. nist.gov
4. CISA
5. VirusTotal
6. MITRE ATT&CK

heimdall
security research
A DIVISION OF ISH

Podcast ISH

Heimdall Security Research