BOLETIM DE SEGURANÇA

CosmicBeetle se une ao RansomHub para lançar o ransomware personalizado ScRansom

heimdall
security research
A DIVISION OF ISH

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

Boletins de Segurança – Heimdall

ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR

ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou cou outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR

ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como Cl0p está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

Sumário

Lista de Tabelas

Lista de Figuras

1 SUMÁRIO EXECUTIVO

Recentemente o grupo de ameaças **CosmicBeetle** desenvolveu uma nova variante personalizada de ransomware, chamada **ScRansom**, que tem sido utilizada em ataques direcionados a pequenas e médias empresas (PMEs) em regiões como **Europa**, **Ásia**, **África** e **América do Sul**. É possível que o grupo esteja atuando como afiliado do **RansomHub**.

2 INFORMAÇÕES SOBRE A AMEAÇA

O CosmicBeetle está ativo desde pelo menos 2020, esse agente de ameaça é mais conhecido pelo uso de sua coleção personalizada de ferramentas Delphi, comumente chamada de Spacecolon, consistindo em ScHackTool, ScInstaller, ScService e ScPatcher. Conforme a ESET, o ScRansom não é um ransomware tecnicamente avançado, mas o CosmicBeetle conseguiu atingir alvos de relevância, provocando prejuízos significativos. Isso é notável especialmente porque o CosmicBeetle ainda é um ator emergente no cenário do ransomware. Durante a implantação do ScRansom, surgem diversos problemas técnicos, o que reflete a inexperiência do grupo. As vítimas que optam por pagar o resgate devem ter cuidado, pois embora o descriptografador funcione adequadamente (até o momento da escrita), frequentemente são necessárias várias chaves de descriptografia. Além disso, há o risco de alguns arquivos se tornarem irrecuperáveis, dependendo da maneira como o grupo realizou o processo de criptografia.

O CosmicBeetle tentou mitigar ou ocultar parcialmente os problemas associados ao seu ransomware ao se passar pelo LockBit, uma das gangues de ransomware mais notórias dos últimos anos. Ao utilizar o nome do LockBit, o CosmicBeetle esperava convencer melhor as vítimas a pagar o resgate. Além disso, o grupo aproveitou o construtor do LockBit Black vazado para gerar amostras personalizadas de ransomware, incluindo notas de resgate em turco. Em investigações, surgiu a hipótese de que o CosmicBeetle possa estar afiliado ao RansomHub, uma nova gangue de ransomware-as-a-service (RaaS) que rapidamente ganhou notoriedade.

A telemetria da ESET revelou diversos casos em que o ScRansom foi implantado em conjunto com outras ferramentas frequentemente utilizadas pelo grupo CosmicBeetle. Além disso, um arquivo ZIP enviado ao VirusTotal incluiu dois arquivos internos, ambos provavelmente relacionados a uma invasão. Esses arquivos contêm amostras do ScRansom, ScHackTool e outras ferramentas associadas ao CosmicBeetle, reforçando as suspeitas. Há também uma grande semelhança de código entre o ScRansom e ferramentas anteriores utilizadas pelo CosmicBeetle, como:

- *Delphi como linguagem de programação*
- *Biblioteca IPWorks para criptografia*
- *Sequências turcas idênticas no código*
- *Uso de espaços após dois pontos em strings, o que rendeu ao conjunto de ferramentas Spacecolon seu nome, e*
- *Semelhança da interface gráfica com o ScHackTool*

3 VETOR DE ACESSO INICIAL E ALVOS

O CosmicBeetle frequentemente utiliza métodos de força bruta e exploração de vulnerabilidades para violação de seus alvos, as seguintes falhas de segurança já foram observadas em exploração pelo ator de ameaça:

- CVE-2017-0144 (EternalBlue)
- CVE-2023-27532 (Vulnerabilidade em um componente Veeam Backup & Replication)
- CVE-2021-42278 e CVE-2021-42287 (Vulnerabilidades de escalonamento de privilégios do AD) por meio do noPac ,
- CVE-2022-42475 (Vulnerabilidade no FortiOS SSL-VPN)
- CVE-2020-1472 (Zerologon)

De acordo com a ESET, pequenas e médias empresas (PMEs) em diversos setores ao redor do mundo são as principais alvos desse grupo de ameaça. Isso ocorre porque essas empresas são mais propensas a utilizar o software vulnerável e, geralmente, não possuem processos eficazes de gerenciamento de patches implementados. Os setores alvos foram os seguintes: Manufatura, produtos farmacêuticos, jurídico, educação, assistência médica, tecnologia, serviços financeiros e governo regional.

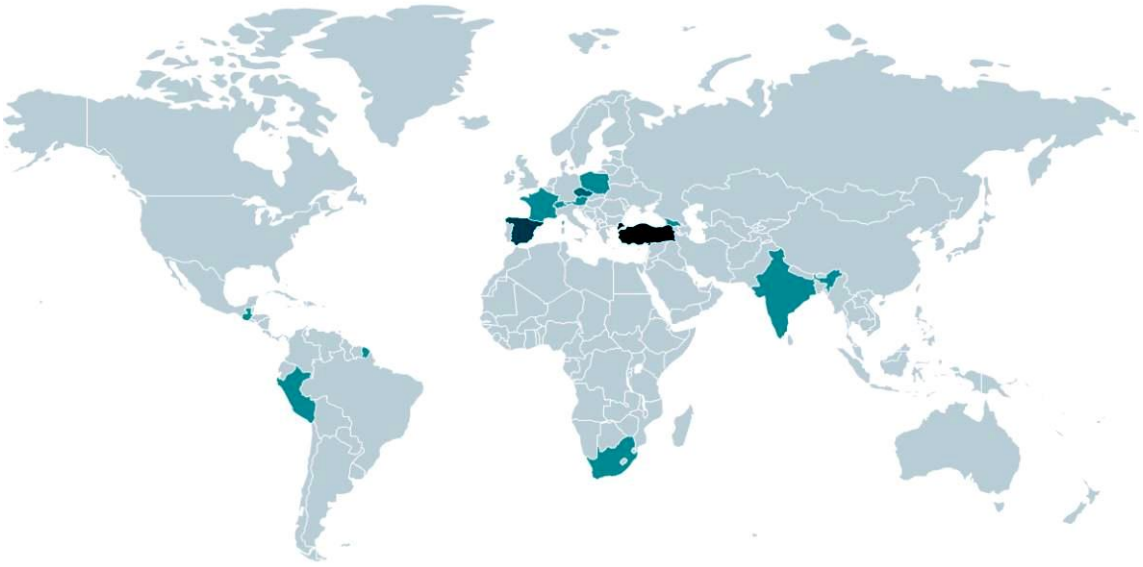

Figura 1 – Mapa de calor dos ataques do CosmicBeetle desde agosto de 2023, de acordo com a telemetria da ESET.

A maioria das notas de resgate deixadas pelo ScRansom não mencionam o nome do ransomware. O grupo CosmicBeetle utiliza principalmente e-mail e o qTox, um aplicativo de mensagens instantâneas bastante popular entre várias gangues de ransomware, principalmente por fazer uso do protocolo Tox. Esse protocolo oferece comunicação criptografada de ponta a ponta entre os envolvidos.

4 CRIPTOGRAFIA DO SCRANSOM

O ScRansom criptografa arquivos em todas as unidades fixas, remotas e removíveis com base em uma lista codificada de extensões, essa lista pode ser modificada por meio da caixa de texto denominada **Extensions**.

Extensões de arquivo direcionadas

*._ms	*.a06	*.bin	*.da3
*.0001	*.accdb	*.bkf	*.da4
*.001	*.ACD	*.bkp	*.danger
*.002	*.adm	*.bkup	*.dat
*.003	*.afi	*.blend	*.db
*.004	*.ai	*.box	*.db1
*.005	*.alt	*.bpf	*.db2
*.006	*.arc	*.btr	*.dbc
*.007	*.arc	*.bup	*.dbdmp
*.008	*.archive	*.c1	*.dbf
.1	*.ard	*.cbd	*.dbs
.2	*.asm	*.cbu	*.dbw
.3	*.avhdx	*.cdr	*.df
*.3dm	*.avi	*.cdx	*.dft
*.3dmbak	*.axf	*.cfgbak	*.diff
*.3ds	*.b1	*.cgd	*.dmp
.4	*.bac	*.couch	*.doc
.5	*.backup	*.csv	*.docx
.6	*.bak	*.ctf	*.dwg
.7	*.BBCK	*.d0	*.dxf
*.7z	*.BBCK3	*.d1	*.dxt5_2d
.8	*.bck	*.d2	*.ebk
.9	*.bco	*.d3	*.edb
*.a01	*.bdmp	*.d4	*.edp
*.a02	*.bi4	*.da1	*.elg
*.a03	*.bik	*.da2	*.eml

*.encvrt	*.ldb	*.ol2	*.qvx
*.fbf	*.ldf	*.old	*.rar
*.fbk	*.llp	*.one	*.raw
*.fbw	*.log	*.ora	*.rbf
*.fdb	*.log1	*.ost	*.rct
*.fmp12	*.lst	*.ostx	*.rdb
*.fp5	*.mat	*.ova	*.redo
*.fp7	*.max	*.pak	*.rfs
*.frm	*.mdb	*.par	*.rman
*.ful	*.mdbx	*.pbd	*.rpd
*.full	*.mdf	*.pcb	*.rpo
*.fxl	*.mmo	*.pdb	*.rpt
*.gan	*.mov	*.pdf	*.rtf
*.gbk	*.mp4	*.pod	*.sai
*.gdb	*.mrimg	*.ppt	*.saj
*.gho	*.msg	*.pptx	*.seq
*.ghs	*.mtx	*.pqb	*.sev
*.hbp	*.myd	*.pri	*.sic
*.hlp	*.myi	*.prt	*.sko
*.hrl	*.nb7	*.psd	*.skp
*.ib	*.nbf	*.psm	*.SLDASM
*.ibd	*.ndf	*.pst	*.SLDDRW
*.idx	*.ndk	*.pstx	*.SLDLFP
*.imd	*.ndx	*.ptb	*.SLDPRT
*.indd	*.nsf	*.qba	*.sldprt
*.itdb	*.nsg	*.qbb	*.sldrpt
*.iv2i	*.ntf	*.qbm	*.slp
*.jet	*.nx1	*.qbw	*.sna
*.jpg	*.nyf	*.qic	*.sna
*.L5X	*.obk	*.qrp	*.spf
*.lbl	*.oeb	*.qsm	*.spl

*.sql	*.tib	*.vct	*.vrb
*.sqlaudit	*.tibx	*.vcx	*.vswp
*.sqlite	*.tif	*.vhd	*.wim
*.sqlite3	*.tiff	*.vhdx	*.wt
*.srd	*.tmp	*.vib	*.xls
*.step	*.trc	*.vix	*.xlsm
*.stm	*.trn	*.vmdk	*.xlsx
*.stp	*.tuf	*.vmsd	*.zip
*.tar	*.upd	*.vmsn	*ibdata
*.tar.gz	*.usr	*.vmx	
*.tga	*.vbk	*.vmxf	
*.tgz	*.vbm	*.vob	

O ScRansom emprega criptografia parcial, onde apenas partes do arquivo são criptografadas. Cinco modos de criptografia são suportados:

- *FAST*
- *FASTEST*
- *SLOW*
- *FULL*
- *ERASE*

Os quatro primeiros modos variam na forma como o ransomware escolhe quais partes do arquivo serão criptografadas. Parece que essa funcionalidade ainda está em fase de desenvolvimento, pois nem todos os modos estão sendo utilizados. Já o último modo, *ERASE*, merece destaque – ao ser aplicado, partes específicas dos arquivos alvo não são criptografadas, mas substituídas por um valor fixo, tornando esses arquivos permanentemente irrecuperáveis. A escolha de qual modo será aplicado a um arquivo é feita por meio dos botões de opção na aba *Actions* ou pela inclusão de sua extensão na aba *Criteria*. Há uma lista de extensões, chamada *Virtual Extensions*, que ativa uma função de criptografia diferente, mas que funciona de forma idêntica à normal. A lista *White Extensions* deve excluir determinadas extensões do processo de criptografia, mas essa função ainda não foi implementada.

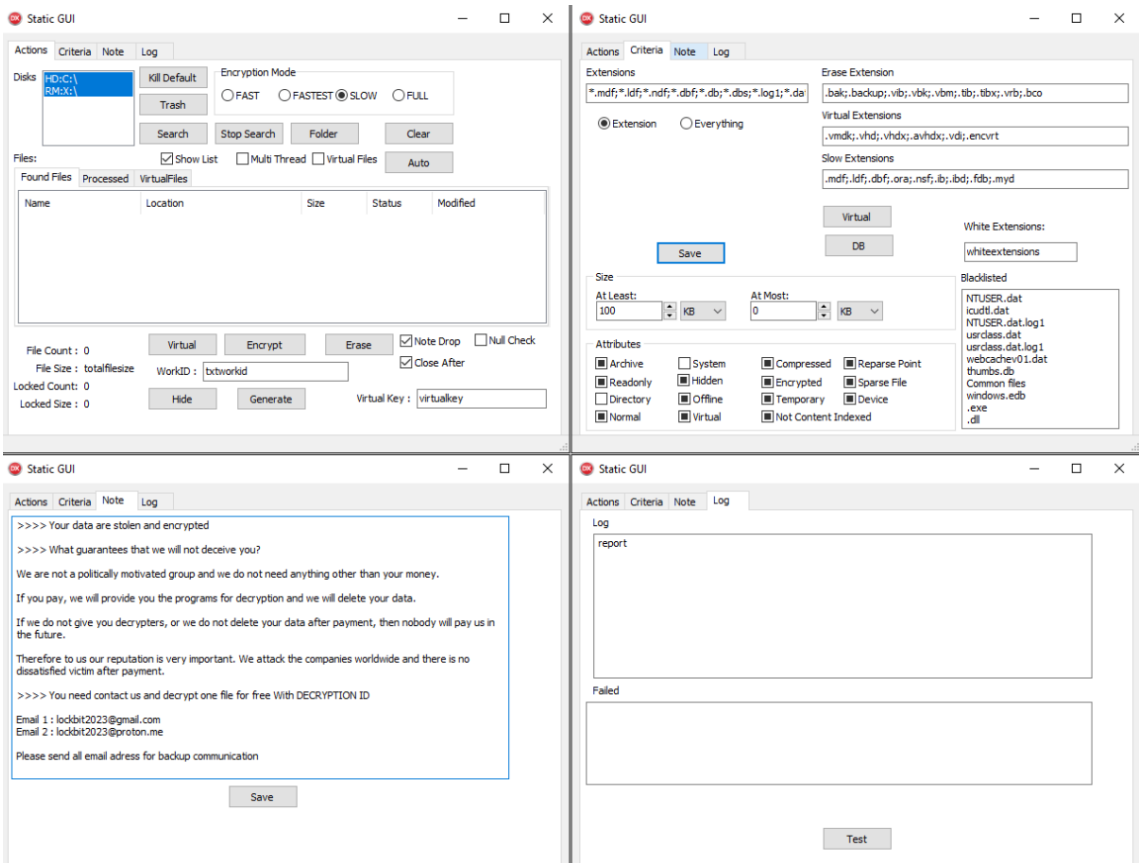

Figura 2 – Interface do usuário do ScRansom.

5 RELAÇÃO COM O RANSOMHUB

A utilização de construtores vazados é uma tática frequentemente empregada por gangues de ransomware menos experientes. Com isso, elas conseguem se aproveitar da reputação de grupos de ransomware mais conhecidos, ao mesmo tempo que obtêm uma amostra funcional do malware. No entanto, a relação com a LockBit não é o único aspecto identificado. Em junho, a ESET analisou um incidente relacionado ao ScRansom. A partir de sua telemetria, foi possível coletar as seguintes informações:

Em 3 de junho de 2024, a CosmicBeetle tentou comprometer uma empresa de manufatura na Índia com a ScRansom. Após falhar, o CosmicBeetle tentou uma variedade de ferramentas de eliminação de processos para remover a proteção EDR, como:

- *Reaper*
- *Darkside*
- *RealBlindingEDR*

Em 8 de junho de 2024, o EDR killer do RansomHub foi executado na mesma máquina. Em 10 de junho de 2024, o RansomHub foi executado na mesma máquina.

A maneira como o EDR killer do RansomHub Ele foi extraído manualmente via WinRAR de um arquivo armazenado em C:\Users\Administrator\Music\1.0.8.zip e executado. Tal execução é muito incomum para afiliados do RansomHub. Por outro lado, usar a pasta Music e extrair e executar manualmente payloads certamente é um comportamento típico do CosmicBeetle. Até onde se sabe, não há vazamentos públicos do código do RansomHub ou de seu construtor (embora o próprio RansomHub provavelmente seja baseado em código comprado da Knight, outra gangue de ransomware). Portanto, acredita-se com confiança média que a CosmicBeetle se inscreveu como um novo afiliado do RansomHub.

6 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Reconnaissance	T1595.002 Active Scanning: Vulnerability Scanning T1590.005 Gather Victim Network Information: IP Addresses	O CosmicBeetle verifica seus alvos em busca de uma lista de vulnerabilidades que ele pode explorar. O CosmicBeetle verifica a internet em busca de endereços IP vulneráveis às vulnerabilidades que ele pode explorar.
Resource Development	T1583.001 Acquire Infrastructure: Domains T1587.001 Develop Capabilities: Malware T1588.002 Obtain Capabilities: Tool T1588.005 Obtain Capabilities: Exploits T1588.001 Obtain Capabilities: Malware	CosmicBeetle registrou seu próprio domínio de site de vazamento. CosmicBeetle desenvolve seu conjunto de ferramentas personalizado, Spacecolon. O CosmicBeetle utiliza uma grande variedade de ferramentas e scripts de terceiros. O CosmicBeetle utiliza PoCs disponíveis publicamente para explorações conhecidas. O CosmicBeetle provavelmente obteve ransomware do RansomHub e do construtor LockBit 3.0 vazado.
Initial Access	T1190 Exploit Public-Facing Application T1204 User Execution	O CosmicBeetle obtém acesso inicial explorando vulnerabilidades no FortiOS SSL-VPN e outros aplicativos públicos. O CosmicBeetle depende da execução do usuário para algumas de suas ferramentas, embora isso geralmente seja feito pelo agente da ameaça via RDP.
Execution	T1059.003 Command and Scripting Interpreter: Windows Command Shell T1059.001 Command and Scripting Interpreter: PowerShell	O CosmicBeetle executa vários scripts e comandos BAT. O CosmicBeetle executa vários scripts e comandos do PowerShell.
Persistence	T1136.001 Create Account: Local Account	O CosmicBeetle geralmente cria uma conta de administrador controlada pelo invasor.
Defense Evasion	T1078 Valid Accounts T1140 Deobfuscate/Decode Files or Information	O CosmicBeetle abusa de contas válidas cujas credenciais ele obtém com sucesso. Amostras do ScRansom protegem chaves RSA públicas por criptografia.
Credential Access	T1110.001 Brute Force: Password Guessing T1212	CosmicBeetle utiliza ataques de força bruta RDP e SMB.

	Exploitation for Credential Access	O CosmicBeetle explora vulnerabilidades conhecidas para obter credenciais.
Impact	T1485 Data Destruction T1486 Data Encrypted for Impact	O CosmicBeetle torna alguns arquivos criptografados irrecuperáveis. O CosmicBeetle criptografa arquivos confidenciais em máquinas comprometidas.

Tabela 1 – Tabela MITRE ATT&CK.

7 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:

Implementação de controle de acesso rigoroso

- **Autenticação multifator (MFA):** Habilitar MFA para todos os usuários, especialmente aqueles com privilégios administrativos, dificulta o acesso não autorizado.
- **Princípio do menor Privilégio:** Limitar os direitos de acesso aos sistemas e dados críticos apenas aos usuários que realmente precisam.

Monitoramento e detecção

- **Soluções de detecção e resposta a ameaças (EDR):** Implementar soluções EDR que possam monitorar atividades incomuns em tempo real e detectar padrões de ataque, como movimentação lateral ou execução de malware.
- **Monitoramento de tráfego de rede:** Utilizar ferramentas de análise de tráfego para identificar comunicações anômalas com servidores de comando e controle (C2) usados pelo grupo.

Backup seguro e segmentado

- **Backups frequentes e seguros:** Realizar backups frequentes e isolados das informações críticas. Os backups devem ser mantidos offline ou em redes segmentadas, de modo a prevenir que sejam criptografados em um ataque de ransomware.
- **Teste de restauração de backups:** Realizar testes periódicos para garantir a integridade e a capacidade de restauração dos backups.

Aplicação de patches e gerenciamento de vulnerabilidades

- **Patching regular:** Manter sistemas, software e servidores atualizados com os últimos patches de segurança. O CosmicBeetle é conhecido por explorar vulnerabilidades conhecidas.
- **Gerenciamento de vulnerabilidades:** Implementar um processo rigoroso de varredura e correção de vulnerabilidades, priorizando aquelas críticas ou ativamente exploradas.

Proteção contra phishing

- **Treinamento de usuários:** Educar os colaboradores sobre os riscos de phishing e como identificar e reportar e-mails suspeitos.

- **Filtragem de e-mail:** Utilizar ferramentas de filtragem avançada de e-mails para bloquear anexos maliciosos e URLs conhecidas por serem usadas em campanhas de phishing.

Segmentação de rede e controle de movimento lateral

- **Segmentação de rede:** Dividir a rede em segmentos para minimizar o impacto em caso de comprometimento de um sistema. Cada segmento deve ter políticas de firewall e controle de acesso específicas.
- **Monitoramento de movimento lateral:** Utilizar ferramentas que detectem movimentos laterais dentro da rede, como tentativas de explorar máquinas vulneráveis após o comprometimento inicial.

Prevenção e mitigação de ransomware

- **Bloqueio de execução de aplicativos não confiáveis:** Implementar políticas de controle de aplicativos que bloqueiem a execução de software não autorizado, limitando o uso de ferramentas de ransomware como o ScRansom.
- **Resposta a incidentes:** Estabelecer um plano de resposta a incidentes para isolar rapidamente sistemas infectados e minimizar o impacto de ataques.

Inteligência de ameaças e atualizações constantes

- **Integração com fontes de inteligência:** Integrar fontes de inteligência de ameaças, como a MISP, para obter informações atualizadas sobre TTPs (táticas, técnicas e procedimentos) usados pelo CosmicBeetle e outros grupos semelhantes.
- **Monitoramento de indicadores de comprometimento (IOCs):** Monitorar e bloquear IOCs associados ao CosmicBeetle, como IPs, domínios e hashes relacionados ao ScRansom.

Criptografia e proteção de dados sensíveis

- **Criptografia de dados:** Garantir que dados sensíveis estejam sempre criptografados em repouso e em trânsito, de forma a evitar o roubo de dados durante um ataque de ransomware.
- **Política de gerenciamento de chaves:** Implementar um sistema de gerenciamento de chaves seguro para proteger as chaves de criptografia usadas na organização.

8 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:	a8570f9c64b9dd0d7e89eeb3327a8c61
sha1:	4497406d6ee7e2ef561c949ac88bb973bdbd214b
sha256:	34e2b621f15ad4747c7e3dde2be3617841ffacba203b93fd2ff3256b914240f7
File name:	ScRansom

Indicadores de compromisso do artefato	
md5:	8404570e27b53d8291f742c1efd15979
sha1:	26d9f3b92c10e248b7dd7be2cb59b87a7a011af7
sha256:	8b67a544d7ddbe8e78fad71aab03431dea585c84a229e6d23832d8f449d47ff2
File name:	New.exe

Indicadores de compromisso do artefato	
md5:	377f6d22b30b79b6cbd850716595fcc4
sha1:	1b635cb0a4549106d8b4cd4edaff384b1e4177f6
sha256:	e44422f6853a2a318f937607e9270ec66a374a3e078d1eedd720f8cb838a165c
File name:	377f6d22b30b79b6cbd850716595fcc4

Indicadores de compromisso do artefato	
md5:	ba2ad45b96907e639853178a571a122d
sha1:	dae100afc12f3de211bff9607dd53e5e377630c5
sha256:	da414697d21874978dcc58930a63c7f2aa42a23b6e8b9580ad4c94d9311c138d
File name:	Project1.exe

Indicadores de compromisso do artefato	
md5:	473aa92db128b6dd772e280eb8facbe5
sha1:	705280a2dcc311b75af1619b4ba29e3622ed53b6
sha256:	87738c63f7098c86625e831ccb7867eca336222bb038fe6411ca4a42186f3cc9
File name:	70880b.msi

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de IPs

Indicadores de IPs	
IP	66.29.141[.]245

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.

9 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **ESET**
- **MITRE ATT&CK**
- **NVD**

10 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH