hardsecure

USE CASE

DARKSIDE

Rua Acácio de Paiva nº 16, 1ºdir,
1700-006 Lisbon, Portugal

www.hardsecure.com
geral@hardsecure.com

INDEX

OBJETIVO

Este documento tem por objetivo apresentar um caso de estudo sobre o ataque de ransomware ocorrido sobre uma empresa americana com algumas evidências de análises e resultados partilhados na comunidade e de empresas de segurança mundialmente reconhecidas.

ENQUADRAMENTO

Este documento tem por objetivo apresentar um caso de estudo sobre o ataque de ransomware ocorrido sobre uma empresa americana com algumas evidências de análises e resultados partilhados na comunidade e de empresas de segurança mundialmente reconhecidas.

O ataque foi confirmado ter sido lançado pelo grupo ciber-criminoso Darkside e acredita-se que tenha sido lançado a partir da Europa de Leste. O ransomware utilizado é relativamente uma nova variante que foi verificado pela primeira vez em agosto de 2020.

Este ataque aos computadores da Colonial Pipeline envolveu ainda o roubo de cerca de 100 GB de dados corporativos. Os dados roubados tornam este ataque ainda mais relevante pelo facto do grupo ter um histórico de extorquir dinheiro duplamente à suas vítimas, não só pedindo dinheiro pelo bloqueio dos dados, e pela negação de serviços afetados, como solicitando pagamentos pelos dados capturados e chantageando divulgar a informação roubada se as vitimas não pagarem. Este modo de operar é inovador que os distingue de outros grupos criminosos como sendo os primeiros a implementar o que se pode referir de ‘serviços de extorsão quádruplos’.

Uns dias antes do ataque, o grupo anunciou que tinham feito mais 3 vítimas noutras geografias como Escócia e Brasil tendo reclamado um roubo 1.9GB de dados, destas 3 companhias, incluindo dados financeiros, dados de clientes, empregados, passaportes e contractos.

Como o Darkside é um RaaS (ransomware-as-a-service), é bem possível que tenham existido 3 grupos associados por detrás destes ataques.

INTEL SOBRE O GRUPO DARKSIDE

O grupo de ransomware Darkside anunciou o seu serviço RaaS em agosto de 2020 por via da imprensa. Desde então tem-se tornado conhecidos pelas suas operações em larga escala. Constroem sistemas de fuga de dados com redundância, efetuam uma análise financeira das vítimas antes do ataque e até proporcionam suporte via web chat às mesmas.

Eles tem declarado publicamente que preferem não atacar hospitais, escolas, organizações sem lucros e governos, mas sim grandes organizações que possam pagar largas somas de resgate.

Análises reversas de código indicam que o malware Darkside verifica pelas definições regionais dos devices atingidos para garantir que não atacam organizações russas. Tem também respondido a questões Q&A em fóruns russos onde se encontram a recrutar ativamente parceiros que falam russo.

O grupo tem ferramentas tanto para sistemas Windows como Linux. Parecido com os grupos NetWalker e REvil, o Darkside tem um programa afiliado que oferece a qualquer um que os ajude a espalhar o seu malware, cerca de 10-25% do lucro.

Baseado em sites TOR de fugas de informação, o grupo Darkside determina se persegue um alvo de uma organização potencial olhando em primeiro lugar para o registo financeiro da mesma. Com isto determina o valor do resgate a solicitar sendo que a soma situa-se entre US$ 2K e US$ 2M.

Relatórios indicam que, baseado nestes sites, haverá pelo menos 90 vítimas afectadas pelo Darkside, num total de mais de 2 TB de informação roubada e armazenada em sites do Darkside, sendo que 100% dos ficheiros das vítimas são libertados publicamente.

Depois do ataque à Colonial Pipeline, o grupo Darkside anunciou num dos seus sites de informação, clarificando que o grupo não deseja criar problemas à sociedade e que o seu objetivo é simplesmente fazer dinheiro. Contudo não há forma de o verificar, sabe-se que o grupo está bastante ativo tal como indicado anteriormente mais 3 vítimas além do Colonial Pipeline.

ANATOMIA DE UM ATAQUE

Darkside é um RaaS (ransomware-as-a-service) que oferece uma percentagem dos lucros aos seus afiliados. Este ransomware é um exemplo da evolução do modelo de negócio, apresentando um modelo moderno em que o ransomware identifica alvos valiosos para potenciar a recompensa pelos ativos comprometidos (como a dupla extorsão). Os ataques modernos de ransomware estão a ser feitos cada vez mais com a colaboração de vários grupos que partilham os lucros, sendo que a tendência é para olhar para este tipo de ataque mais como ameaças avançadas persistentes (APT) do que eventos isolados de ransomware, como passamos a descrever.

Aqui estão alguns exemplos da atividade deste grupo em relatórios públicos divulgados:

- August 2020: DarkSide introduces its ransomware.
- October 2020: DarkSide donates US$20,000 stolen from victims to charity.
- November 2020: DarkSide establishes its RaaS model. The group invites other criminals to use its service. A DarkSide data leak site is later discovered.
- November 2020: DarkSide launches its content delivery network (CDN) for storing and delivering compromised data.
- December 2020: A DarkSide actor invites media outlets and data recovery organizations to follow the group's press center on the public leak site.
- March 2021: DarkSide releases version 2.0 of its ransomware with several updates.
- May 2021: DarkSide launches the Colonial Pipeline attack. After the attack, Darkside announces it is apolitical and will start vetting its targets (possibly to avoid raising attention to future attacks).

Táticas de evasão incluem:
- Command and control sobre TOR
- Evitam pontos onde software EDR está a correr
- Períodos de espera longos para ações mais ruidosas para os passos tardios seguintes
- Técnicas de ofuscação como carregamento dinâmico de bibliotecas e codificação
- Técnicas anti forenses e anti-debugging como eliminação de logs

Passos na sequência de ataque envolvem:
- Recolha de credenciais de ficheiros memória em domain controllers
- Uso de file shares para distribuir ferramentas de ataquem e arquivamento de ficheiros
- Relaxamento de permissões no file shares para facilidade da extração
- Eliminação de backups e shadow copies (VSS)
- Disseminação de ransomware

ACESSO INICIAL

O ransomware Darkside tem a particularidade de se adaptar ao ambiente das suas vítimas, sendo que tem disso visto explorando vários vetores de ataque como phishing, abuso de protocolo RDP (remote desktop protocol) e explorando vulnerabilidades e táticas para ganhar acesso inicial. Várias ferramentas legítimas podem ser usadas no processo para permanecerem como atividades normais passando despercebidas pelas defesas e ofuscando o ataque. Ganhar acesso inicial pelos elos mais fracos como contas e sistemas remotamente exploráveis.

Algumas ferramentas de reconhecimento e entrada que tem sido vistas:
- Powershell: reconhecimento
- Metasploit: reconhecimento
- Mimikatz: reconhecimento
- BloodHound: reconhecimento
- Cobalt Strike: Instalação

Estes ataques modernos do grupo Darkside servem para ganhar acesso, não significa que o ransomware seja de imediato largado e executado pelos atacantes.

Os atacantes estabelecem ligações command and control primariamente através de cliente RDP sobre porta 443, roteado através de rede TOR. Depois da instalação do TOR browser, eles modificam a configuração para correr como um serviço persistente, redirecionando o tráfego para uma porta local dinâmica por TOR via HTTPS sobre porta 443, ou seja, acaba por ser praticamente indistinto o tráfego de um acesso normal web. Estas ligações são persistentes para que os atacantes possam estabelecer sessões RDP sobre sistemas comprometidos, facilitando o movimento lateral.

Os atacantes usam Cobalt Strike como um mecanismo secundário de command and control. Foram observados vários ficheiros de etapa customizados (ex: file.exe) que efetuam downloads de beacons ligados a servidores específicos. Estes ficheiros são disseminados remotamente em dispositivos alvo pelo WinRM. Estes ficheiros estabelecem ligações a servidores C2 dedicados para efectuar o download do Cobalt Strike Beacon.

Normalmente outros grupos usam poucos servidores C2 por vítima, mas o Darkside configura cada beacon para ligar a servidores C2 diferentes por cada agente. Isto é indicador que o grupo opera a uma escala enorme, com uma infraestrutura bem estabelecida.

Os ficheiros de etapa e executáveis TOR são armazenados em áreas de rede partilhadas para uma distribuição fácil. Os atacantes evitam a instalação de backdoors em sistemas monitorizados por soluções EDR.

Foram observados que os atacantes logam-se nos ambientes VDI com várias contas, muitas vezes concorrentemente. De cada vez que um atacante se loga, ficheiros .lnk são criados nas pastas dos utilizadores comprometidos. Estes ficheiros .lnk ajudam a determinar que contas e outros ambientes VDI tem sido comprometidos e quando cada conta foi usada no ataque.

RECONHECIMENTO, MOVIMENTO LATERAL E ESCALAMENTO DE PRIVILÉGIOS

Este processo é chave no processo de mapeamento da organização, tal como outro tipo de ataques avançados, sendo que o objetivo é identificar dados críticos na organização da vítima, ficheiros alvo e localizações para poder extrair dados e passos seguintes de cifrar dados.

Tem sido reportado que no caso do Darkside, os relatórios confirmam que o objetivo do movimento lateral é ganhar acesso ao Domain Controller e à AD, usando credenciais roubadas e escalamento de privilégios. Alguns dos métodos utilizados para o efeito com mínimo de capacidade de deteção e bloqueio empregam o uso de advanced_ip_scanner.exe, PSExec, mimikatz e RDP e métodos normalmente associados a grupos APT, adaptando as ferramentas e métodos às defesas da vítima.

Dos hosts comprometidos, verificam-se pedidos de kerberos, ligações NTLM para ganhar acesso adicional a sistemas e contas. Depois de algum período de tempo os atacantes usam uma ferramenta powershell de reconhecimento na AD (ADRecon.ps1) para obter informações sobre utilizadores, grupos, privilégios, recursos e armazenam os resultados num ficheiro DC.txt. Cada um dos ataques realizados pelas ferramentas são apagados depois de utilizados. O atacante armazena temporariamente os resultados do reconhecimento e informação de credenciais num servidor Windows com muita atividade. Vários ficheiros são escritos e apagados no servidor, tais como Typed_history.zip, Appdata.zip, IE_Passwords.zip, AD_intel e ProcessExplorer.zip.

Em adição ao roubo de credenciais, os atacantes recolhem credenciais dos perfis dos utilizadores incluindo:
- Users\<user name>\Appdata\[Roaming\Local]\Microsoft [Credentials\Vault]
- Users\<user name>\Appdata\Roaming\Mozilla\Firefox\Profiles
- Users\<user name>\\Appdata\Local\Google\Chrome

Os atacantes executam Invoke-mimikatXz.ps1 para extrair credenciais de servidores não monitorizados e guardam-nas num ficheiro chamado dump.txt. Esta operação é realizada num alvo de elevado perfil com o mínimo de capacidade deteção.

O atacante quando obtêm credenciais de domain admin acedendo a domain controllers, em fases avançadas do ataque, realizam o conhecido ataque DCsync em que passam a ter um domain controller legitimo e utilizam o serviço de replicação da AD (Directory Replication Service) para acederem e recolherem dados de passwords de todo o domínio, incluído hashes de kerberos.

RECOLHA DE DADOS, STAGING E EXFILTRAÇÃO

Esta prática de extorsão associada à exfiltração de dados é o passo mais arriscado tendo maior probabilidade de ser detetado pelas equipas de segurança da organização. Contudo é normalmente o último passo do ataque antes do lançamento do ransomware e o ataque acelera a partir deste ponto até ser concluído.

Algumas ferramentas em uso neste processo:
- 7-zip: arquivo de ficheiros
- Rclone e Mega: ferramentas usadas para exfiltração de ficheiros para espaço em cloud
- Putty: aplicação alternativa para transferência de ficheiros na rede

O servidor Windows com muita atividade, serve de hub (central) para armazenar dados antes da exfiltração. Dados recolhidos de centenas de servidores com uma rotina batch (dump.bat) localizado em \Desktop\Dump, escreve ficheiros para a mesma localização, comprimindo-os em ficheiros 7zip com uma nomenclatura padrão simples convencional *.7z.[001]-[999].

Apesar de terem acumulado privilégios elevados, observa-se que os atacantes relaxaram as permissões nos File Systems, alargando-as ao acesso de qualquer conta de utilizador de domínio. O ficheiro batch recolhe dados e os arquivos são eliminados pelos atacantes horas depois da extração.

O grupo Darkside usa vários sites de fuga de dados baseados em TOR para armazenarem os dados roubados. Entre os sites usados para a exfiltração de dados incluem-se Mega e PrivatLab.

CIFRAGEM

O Darkside não emprega o ransomware enquanto não tiverem o ambiente mapeado, extraído dados de interesse, ganho controlo e privilégios e identificado todos os sistemas de backup, servidores e aplicações. Tem sido observado ligações a repositórios de backup principais utilizando contas de serviço comprometidas imediatamente antes da cifragem dos dados. Por aguardarem pela fase de cifragem do ataque, os atacantes colocam-se numa posição maximizada de dano e lucro.

A execução do ransomware ocorre a seguir. O Darkside partilha muitas semelhanças com o REvil nesta etapa do processo, incluindo a estrutura das notas de regaste, uso de powershell e a execução de comandos para eliminar shadow copies da rede.

Adicionalmente ao PowerShell utilizado para instalar e operar o malware, o grupo utiliza Certutil e Bitsadmin para descarregar o ransomware. São utilizados 2 métodos de cifra nas comunicações, dependendo do sistema operativo alvo (Windows ou Linux). Usam cifra ChaCha20 com RSA-4096 em Linux e Salsa20 com RSA-1024 em Windows. O código ransomware é entregue pelas backdoors estabelecidas (TOR-RDP ou Cobalt Strike) e customizadas a cada vitima. O payload inclui o executável, uma extensão única, um ID único da vitima para que a mesma possa aceder ao site do Darside e efetuar o pagamento.

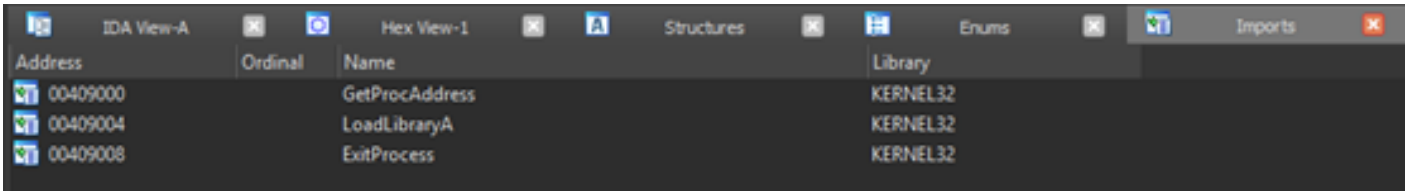
Por utilizar executáveis e extensões únicos, o ransomware evita mecanismos de defesa por assinatura facilmente.

ETAPAS DO RANSOMWARE DARKSIDE

ETAPA 1 - INJEÇÃO

Na execução por comando CMD, o malware copia-se para o caminho "C:\Users\admin\AppData\Local\Temp\" e injeta o seu código num processo existente. Se o malware encontra indicações de que está a ser analisado ou a correr numa VM, ele pára imediatamente.

Para evitar a deteção por AV e EDR, o ransomware carrega dinamicamente as suas bibliotecas sem as registar na sua secção de importação.



Apenas 3 bibliotecas são importadas, o que indica que outros nomes de bibliotecas são resolvidos dinamicamente durante a execução do malware.

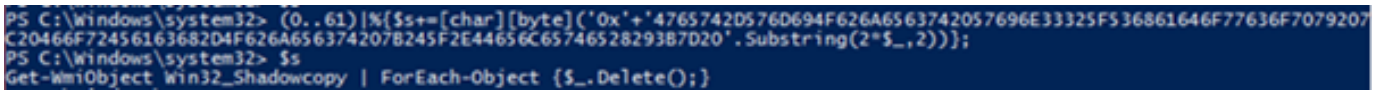
ETAPA 2 - ELIMINAÇÃO DE SHADOW COPIES

Utilizando um PowerShell ofuscado, o malware tenta eliminar as shadow copies do dispositivo da vítima.

Comando ofuscado:

```
powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]
('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F724561636 82D4
F626A6563742078245F2E44656C6574652829 3B7D20'.Substring(2*$_,2))};iex $s"
```

Comando ofuscado:



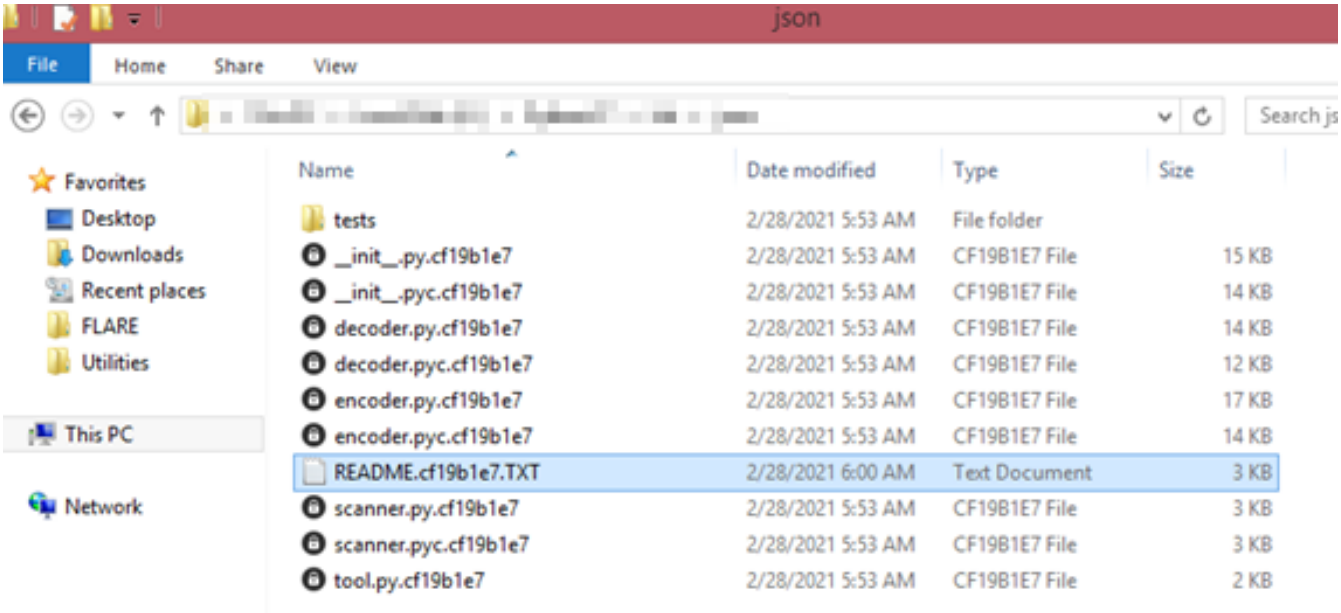
ETAPA 3 - CIFRAGEM DOS DADOS

AfDepois da eliminação das shadow copies, o malware termina processos específicos para evitar que existam ficheiros bloqueados e que atrasem a cifragem, e inicia a sua rotina.

Lista de processos:
- Sql
- Oracle
- Ocssd
- Dbsnmp
- Synctime
- Agntsvc
- Isqlplussvc
- Xfssvccon
- Mydesktopservice
- Ocautoupds
- Encsvc
- Firefox
- Tbirdconfig
- Mydesktopqos
- Ocomm
- dbeng50
- sqbcoreservice
- excel
- infopath
- msaccess
- mspub
- onenote
- outlook

- powerpnt
- steam
- thebat
- thunderbird
- visio
- winword
- wordpad
- notepad

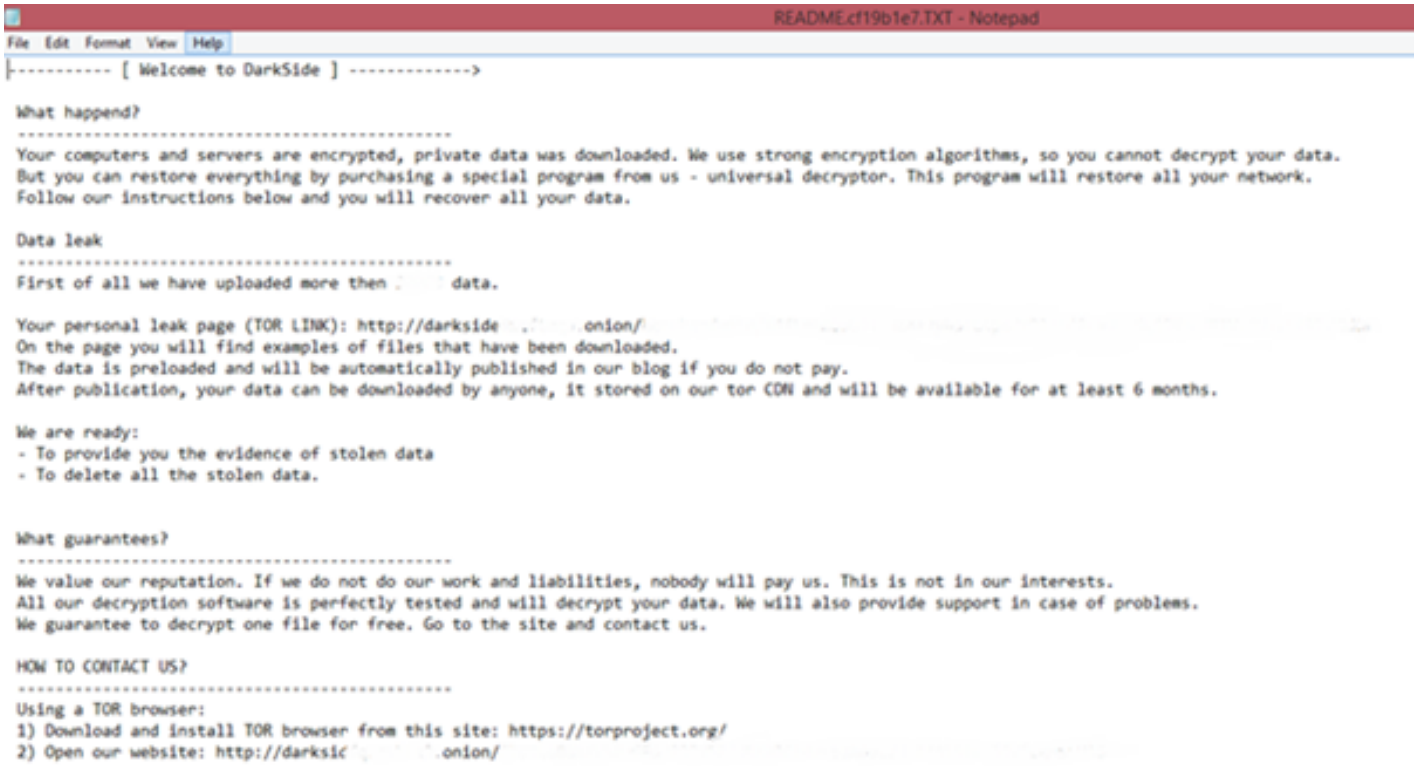
Durante a cifragem, o malware adiciona 8 caracteres ao final do nome do ficheiro cifrado:



O ransomware evita cifrar ficheiros com as seguintes extensões:

386, adv, ani, bat, bin, cab, cmd, com, cpl, cur, deskthemepack, diagcab, diagcfg, diagpkg, dll, drv, exe, hlp, icl, icns, ico, ics, idx, ldf, lnk, mod, mpa, msc, msp, msstyles, msu, nls, nomedia, ocx, prf, ps1, rom, rtp, scr, shs, spl, sys, theme, themepack, wpx, lock, key, hta, msi, pdb

Cria um ficheiro README...TXT com instruções para contactar o criador do ransomware para a decifragem:


README.cf19b1e7.TXT - Notepad

File Edit Format View Help

---------- [Welcome to DarkSide] ------------>

What happend?

Your computers and servers are encrypted, private data was downloaded. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak

First of all we have uploaded more then data.

Your personal leak page (TOR LINK): http://darkside onion/
On the page you will find examples of files that have been downloaded.
The data is preloaded and will be automatically published in our blog if you do not pay.
After publication, your data can be downloaded by anyone, it stored on our tor CDN and will be available for at least 6 months.

We are ready:
- To provide you the evidence of stolen data
- To delete all the stolen data.

What guarantees?

We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

HOW TO CONTACT US?

Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksi onion/

É interessante verificar que a nota que o Darkside deixa é semelhante a do Babuk, o que deixa a indicação de que estas 2 famílias de malware partilham um link.

MITRE ATT&CK

Os TTPs associados ao Darkside:

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
T1590 (Gather Victim Network Information)	T1078 (Valid Accounts)	T1059.004 (Command and Scripting Interpreter: Unix Shell)	T1078 (Valid Accounts)	T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)	T1222.002 (File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification)	T1555 (Credentials from Password Stores)
	T1566 (Phishing)	T1059.001 (Command and Scripting Interpreter: PowerShell)	T1053 (Scheduled Task/Job)	T1036 (Masquerading)	T1214 (Credentials in Registry)	T1082 (System Information Discovery)
	T1190 (Exploit Public-Facing Application)	T1569 (System Services)	T1098 (Account Manipulation)	T1140 (Deobfuscate/Decode Files or Information)	T1083 (File and Directory Discovery)	T1071 (Standard Application Layer Protocol)
					T1055 (Process Injection: Dynamic-link Library Injection)	T1057 (Process Discovery)
					T1500 (Compile After Delivery)	T1555.003 (Credentials from Password Stores: Credentials from Web Browsers)
					T1562.001 (Impair Defenses: Disable or Modify Tools)	

Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1087 (Account Discovery)	T1080 (Taint Shared Content)	T1113 (Screen Capture)	T1043 (Commonly Used Port)	T1567.002 (Exfiltration Over Web Service: Exfiltration to Cloud Storage)	T1489 (Service Stop)
T1105 (Remote File Copy)	T1486 (Data Encrypted for Impact)			T1048 (Exfiltration Over Alternative Protocol)	T1214 (Credentials in Registry)
T1490 (Inhibit System Recovery)					T1083 (File and Directory Discovery)
T1105 (Ingress Tool Transfer)					T1055 (Process Injection: Dynamic-link Library Injection)
T1087.002 (Account Discovery: Domain Account)					T1500 (Compile After Delivery)
T1482 (Domain Trust Discovery)					T1562.001 (Impair Defenses: Disable or Modify Tools)
T1069.002 (Permission Groups Discovery: Domain Groups)					
T1018 (Remote System Discovery)					
T1016 (System Network Configurartion Discovery)					

CONCLUSÃO

O grupo tem continuado a ser uma ameaça persistente e permanente, evoluído o modelo de ransomware. Este modelo mudou em vários aspetos, conforme o Darkside demonstra pelas suas atividades. Alvos maiores, técnicas avançadas de extorsão alcançando maiores consequências para além das próprias vítimas.

Os grupos de ransomware não estão apenas satisfeitos com bloquear dados nos computadores das vitimas e pedir um resgate. Agora estão a penetrar fundo nas redes das vítimas alcançado novas formas de potenciar e alcançar lucro das suas atividades.

No ataque à Colonial Pipeline, o Darkside usou extorsão dupla. Mas alguns atores foram ainda mais longe, conforme indicado pelas fases de ransomware:

Fase 1: Apenas ransomware.

Fase 2: Dupla extorsão, fase 1 + exfiltração de dados.

Fase 3: Tripla extorsão, fase 1 + 2 + ameaça de DDoS.

Fase 4: Quadrupla extorsão, fase 1 + (outras fases) + contactam diretamente os clientes da vitima ou através de serviços contratados de cal centres para os contactos.

É um claro sinal que existe de facto uma evolução e inovação neste tipo de ataques, sendo que o ransomware apenas irá continuar a evoluir. As organizações tem de se preparar e por em prática um plano de resposta a incidentes focado no novo modelo de ataques de ransomware. Neste ataque à Colonial Pipeline foi verificado por peritos de segurança que a empresa corria uma versão vulnerável do Microsoft Exchange entre outras falhas de segurança. Um ataque a uma empresa desta dimensão pode causar efeitos disruptivos que prejudicam vários sectores da sociedade, como tal, proteger estes serviços é uma prioridade fundamental.

RECOMENDAÇÕES

Por forma a minimizar o risco de exposição ciber ataques, recomenda-se a quem possa interessar a leitura deste artigo:

- É fundamental garantir implementadas boas práticas na gestão da informação interna, e reduzir a exposição digital desnecessária. Muitos casos de serviços que são descontinuados e esquecidos pelas empresas, deixando sistemas vulneráveis expostos externamente, que facilmente podem ser explorados por atores maliciosos para intrusão na rede de uma organização, passando o perímetro de segurança e colocando em risco toda a rede de serviços, utilizadores e sistemas.

- Garantir a atualização regular de sistemas operativos, sistemas de defesa (por ex. antivírus), aplicações, bases de dados, web servers e frameworks para que vulnerabilidades recentes existentes sejam mitigadas. Todos os meses são descobertas novas vulnerabilidades e torna-se fundamental garantir estas atualizações periódicas num período curto de tempo (mensalmente).

- Implementar backups regulares, controlo, testes e resiliência dos sistemas. Os backups são o último recurso num ataque de ransomware efetivo em que não exista forma de recuperação dos dados por decifragem dos mesmos (maioria da recuperação de casos de ransomware depende de backups). Estes sistemas são ativos de importância elevada e devem ser segregados os seus acessos das redes de utilizadores e devem ser testados regularmente.

- Garantir a segmentação e segregação das redes quer fisicamente e logicamente de forma adequada a garantir que a informação privilegiada se encontra protegida por camadas de acessos e se situa no ponto mais restrito e controlado da rede da organização. Esta segregação visa proteger as redes de dados das redes de utilizadores e minimizar a disseminação de malware.

- Ter uma política de segurança da informação implementada, regularmente atualizada e posta efetivamente em prática por equipas de auditoria e compliance nas suas vertentes humana, departamental, tecnológica, física e logica, englobando pelo menos os temas:
  - I. Política de controlo de acessos.
  - II. Política de BYOD.
  - III. Procedimentos de gestão de incidentes.
  - IV. Política de gestão de alterações.
  - V. Política de atualização de Sistemas de Informação.
  - VI. Política de gestão de vulnerabilidades.
  - VII. Política de Backups.
  - VIII. Política de treino e formação de colaboradores.

- As ações de treino, formação e 'awareness' continua dos colaboradores da organização para que identifiquem eficientemente possíveis ameaças disseminadas por campanhas de phishing. As ações dos utilizadores são muitas vezes por desconhecimento despoletadas por malwares iniciais que o utilizador corre inadvertidamente colocando todo um sistema de informação em causa.

- Ter equipas internas ou serviços de cibersegurança contratados como o serviço de resposta a incidentes com profissionais experientes e qualificados, para a implementação de controlos e monitorizações sobre a infraestrutura de rede e ativos de importância e prioridade elevada:
  - I. Estas equipas podem implementar sistemas de monitorização da rede como IDS/IPS, SIEM e configurar logs e controlos sobre a rede e os assets valiosos da empresa para rastreio e proteção.
  - II. Serviço contínuo de monitorização e resposta a incidentes 24x7 sobre a rede de dados.
  - III. Avaliar ameaças e identificação de vulnerabilidades alvo de mitigação.
  - IV. Recomendar alterações ou implementações com vista a reduzir a exposição digital desnecessária.

- Implementar restrições e requisitos de utilizadores e passwords nos sistemas e rede de sistemas:
  - I. Mínimo de 14 caracteres alfanuméricos e caracteres especiais.
  - II. Expiração de passwords a cada 30 dias.
  - III. Limite de histórico de passwords restrito a 20.
  - IV. Implementação de MFA.
  - V. Restrição do nr. de administradores na organização.
  - VI. Configuração de utilizadores nominais.
  - VII. Utilizadores aplicacionais apenas para serviços com passwords de 20 caracteres mínimo com mesma complexidade e aplicação de plano de restrição temporal para atualização das mesmas (1 ano).

- Desativar serviços partilhados de Ficheiros e Impressoras. Se forem necessários, utilizar passwords fortes (idêntico a utilizadores aplicacionais). Implementar mesma complexidade ao nível da AD. - Hardening

- Implementar protocolos seguros (por ex. SMBv 2 e 3, NTLMv2, HTTPs) e desativar protocolos inseguros ou vulneráveis (SMBv1, LM, NTLMv1, HTTP) - Hardening

- Implementar criptografia moderna (TLS1.2 e 1.3), desativar protocolos vulneráveis dos sistemas (SSL < 3.0, TLS < 1.2), desactivar cifras vulneráveis (RC2, RC4, DES, 3DES, MD5, NULL) - Hardening

- Ativar auditoria centralizada da AD sobre processos e serviços e de syslog centralizado

No caso do ransomware em análise, a redução das vulnerabilidades externas indicadas por atualização dos sistemas, poderia ter evitado a exploração de vulnerabilidades diretas relacionadas com protocolo RDP e Exchange. Nunca desvalorizando a ameaça, poderia dificultar o trabalho do grupo em questão, mas é importante salientar que o mesmo atua sobre vários tipos de vetores de possível ataque (por ex. ataques de phishing) em que se torna necessário ter uma vigilância ativa e permanente dos controlos que venham a ser implementados sobre os fluxos e redes de dados.