2021/07

RANSOMWARE NA DARKWEB

AKO
ASTRO TEAM
AVADDON
BABUK LOCKER
CLOP
CONTI
CUBA
DARKSIDE
DOPPELPAYMER
EGREGOR
EVEREST
GRIEF
HIVE
LOCKBIT
LORENZ
LV
MARKETO
MAZE
MOUNT LOCKER
N3TWORM
NEFILIM
NEMTY
NETWALKER
NONAME
PAY2KEY
PAYLOAD.BIN
PROMETHEUS
PYSA
RAGNAR_LOCKER
RAGNAROK
RANSOMEXX
RANZY LOCKER
SEKHMET
SODINOKIBI (REVIL)
SUNCRYPT
SYNACK
TEAM SNATCH
VICE SOCIETY
XING LOCKER

apura

EVOLUÇÃO DA AMEAÇA

1989

Apesar de ter ganhado os holofotes nos últimos anos, os ransomwares já existem há bastante tempo. Em suas versões iniciais, ainda nos anos 1980, não passava de um incômodo, pois além de utilizar códigos de encriptação fracos, as solicitações de “resgate” eram de algumas poucas centenas de dólares.

2013

Foi em 2013 que surgiu a primeira amostra verdadeiramente perigosa de ransomware. Chamada CryptoLocker, utilizava encriptação de nível militar e a chave era armazenada em um servidor remoto, praticamente impossível de ser recuperada sem o pagamento do valor exigido.

2017

Em 2017, a amostra WannaCry ganhou notoriedade ao fazer dezenas de milhares de vítimas em todo mundo, explorando a vulnerabilidade EternalBlue nos sistemas Windows, que permitia execução remota de código. Essa vulnerabilidade teria sido supostamente vazada da NSA (Agência de Segurança Nacional dos EUA).

2018

Mas foi no final de 2018, com o surgimento do Ryuk, que os ransomwares começaram a se espalhar de forma mais intensa, ganhando cada vez mais amostras e fazendo mais e mais vítimas dos diversos setores em todos os continentes. Os operadores por detrás das ameaças passaram a se organizar, a se profissionalizar, fazendo dos ransomwares um verdadeiro negócio.

O serviço online e gratuito "ID Ransomware", que ajuda a catalogar e identificar amostras de ransomware, aponta atualmente a existência de cerca de 1015 amostras diferentes. E novas surgem todos os dias. Códigos-fonte de ransomwares são vendidos ou compartilhados livremente em fóruns underground possibilitando que até mesmo pessoas com pouco conhecimento técnico criem suas próprias variantes.

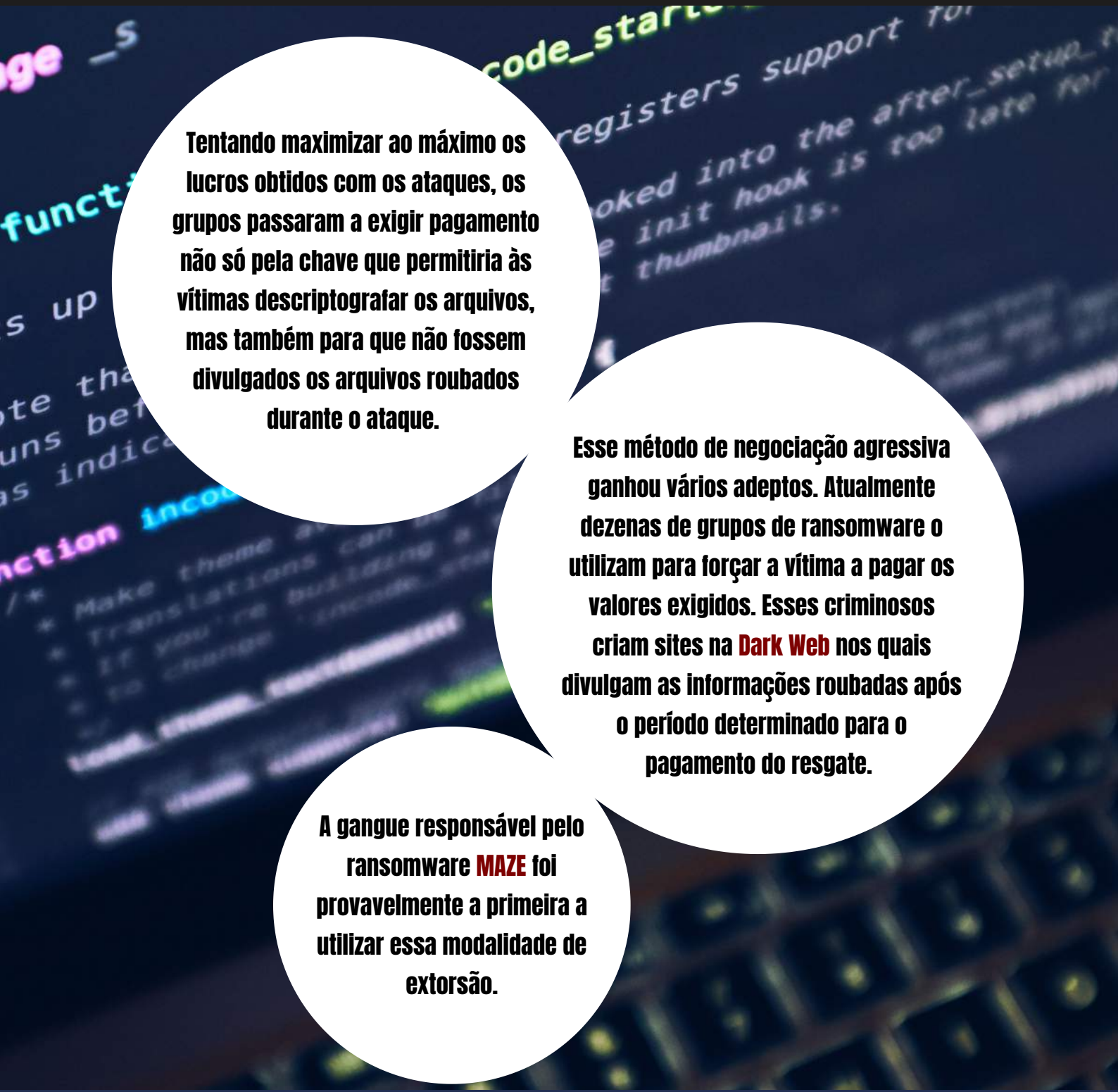
Ransomware as a Service

RaaS

A maioria dos grandes grupos responsáveis por ransomwares na atualidade operam no modelo Ransomware-as-a-Service (RaaS), ou seja, eles oferecem àqueles que chamam de afiliados a oportunidade de usar a amostra que eles desenvolveram em troca de uma comissão. Normalmente os operadores ficam com 30% e os afiliados com 70% dos valores extorquidos das vítimas.

Dessa forma, os grupos conseguem maximizar o faturamento ao mesmo tempo em que minimizam os riscos, tendo em vista que os afiliados ficam responsáveis por toda parte operacional, isto é, invadir os sistemas das vítimas e implantar o ransomware. Os operadores se ocupam exclusivamente de negociar os valores e recebê-los, fazendo depois a partilha com os afiliados.

DUPLA EXTORSÃO



Tentando maximizar ao máximo os lucros obtidos com os ataques, os grupos passaram a exigir pagamento não só pela chave que permitiria às vítimas descriptografar os arquivos, mas também para que não fossem divulgados os arquivos roubados durante o ataque.

Esse método de negociação agressiva ganhou vários adeptos. Atualmente dezenas de grupos de ransomware o utilizam para forçar a vítima a pagar os valores exigidos. Esses criminosos criam sites na **Dark Web** nos quais divulgam as informações roubadas após o período determinado para o pagamento do resgate.

A gangue responsável pelo ransomware **MAZE** foi provavelmente a primeira a utilizar essa modalidade de extorsão.

LGPD

Com a implementação de legislação de proteção de dados em vários países, como por exemplo a recém aprovada Lei Geral de Proteção de Dados (LGPD) no Brasil, os ataques de ransomware tendem a se intensificar. Os criminosos se valem da existência desses mecanismos legais para tentar forçar as vítimas a pagarem os resgates, contando com o medo de sanções e multas decorrentes dessas leis.

NA DARK WEB

As gangues de ransomware mais ativas começaram a utilizar sites na Dark Web para expor suas vítimas e, assim, forçarem-nas a pagar os valores exigidos. A partir dessas postagens é possível fazer uma análise sobre as vítimas, países mais atingidos, longevidade dos grupos, etc.

A análise realizada não pretende traçar um perfil fechado e definitivo, apenas um instantâneo da atividade dos grupos de ransomware e seus afiliados.

Para compor os dados deste relatório, foram utilizados como ponto de partida as informações da planilha criada e mantida pela empresa de cibersegurança Darktracer na qual são listadas as vítimas dos ransomwares, o grupo responsável pelo ataque e a data em que a informação foi postada no site da Dark Web. Foram utilizados os dados postados na planilha até o dia 30 de junho de 2021.

Esses dados foram enriquecidos com informações de área de atuação da empresa vítima e o país em que a empresa se encontra. Para facilitar a exposição dos dados, foram utilizadas como áreas de atuação dezoito categorias, sendo elas: **Advocacia**; **Alimentos/Bebidas**; **Automóveis**; **Combustível**; **Comunicação**; **Educação**; **Energia**; **Engenharia/Arquitetura**; **Finanças**; **Indústria/Manufatura**; **Saúde**; **Setor Público**; **Tecnologia**; **Transporte/Logística**; **Turismo/Hotelaria**; **Varejo/Atacado**; **Moda** ; e **Outros**.

Na categoria **Outros**, estão empresas que não se encaixam nas demais, como por exemplo prestação de serviços diversos, empresas de contabilidade/contadores, imobiliárias, empresas do ramo de diversão, etc.

NO MUNDO: 2573 EMPRESAS

Ao todo 2573 empresas de todos os setores em todo o mundo tiveram informações publicadas nos sites dos operadores de ransomware identificados, no período.

Estados Unidos	1346
Canadá	171
França	129
Reino Unido	124
Alemanha	100
Itália	89
Brasil	69
Austrália	47
Espanha	41
Índia	31
Japão	22
Suíça	17
México	16
UAE	17
África do Sul	14
Áustria	10
Suécia	10

Indústria/Manufatura	473
Outros	254
Tecnologia	227
Engenharia/Arquitetura	226
Saúde	188
Varejo/Atacado	168
Finanças	131
Alimentos/Bebidas	124
Transporte/Logística	117
Setor Público	116
Advocacia	108
Educação	103
Automóveis	61
Comunicação	45
Energia	38
Moda	35
Combustível	31
Turismo/Hotelaria	28
Indefinido	100

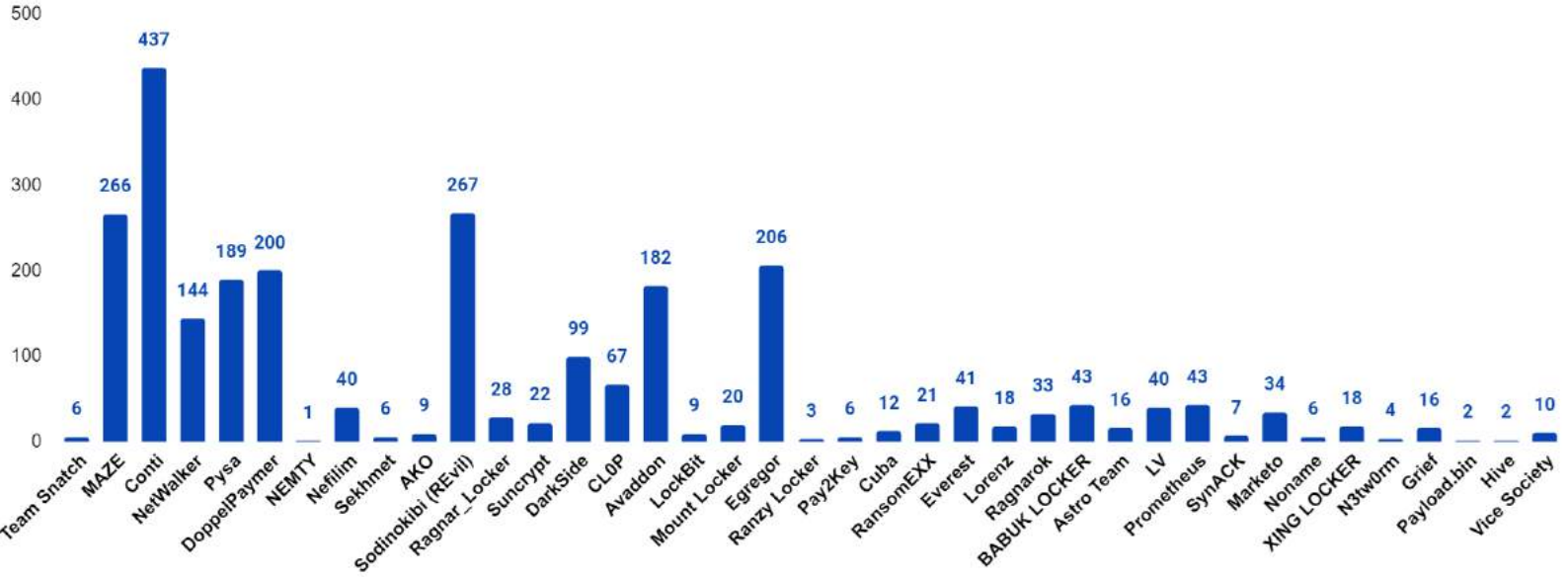
Mais de 90 países tiveram empresas com informações divulgadas na darkweb

Foram identificados pelo menos 39 grupos de ransomware que criaram e mantiveram, em algum momento, site em que publicavam informações roubadas das vítimas.

Conti	437
Sodinokibi (REvil)	267
MAZE	266
Egregor	206
DoppelPaymer	200
Pysa	189
Avaddon	182
NetWalker	144
DarkSide	99
CLOP	67
BABUK LOCKER	43
Prometheus	43
Everest	41
Nefilim	40
LV	40
Marketo	34
Ragnarok	33
Ragnar_Locker	28
Suncrypt	22
RansomEXX	21

Mount Locker	20
Lorenz	18
XING LOCKER	18
Astro Team	16
Grief	16
Cuba	12
Vice Society	10
AKO	9
LockBit	9
SynACK	7
Team Snatch	6
Sekhmet	6
Pay2Key	6
Noname	6
N3tworm	4
Ranzy Locker	3
Payload.bin	2
Hive	2
NEMTY	1

Ocorrências de ransomware pela ordem em que a amostra foi identificada na Dark Web



GRUPOS DE RANSOMWARE MAIS ATIVOS E ÁREAS DE ATUAÇÃO MAIS ATACADAS

CONTI

- 17% Indústria/ Manufatura
- 13% Outros
- 9% Engenharia/ Arquitetura
- 9% Varejo/ Atacado

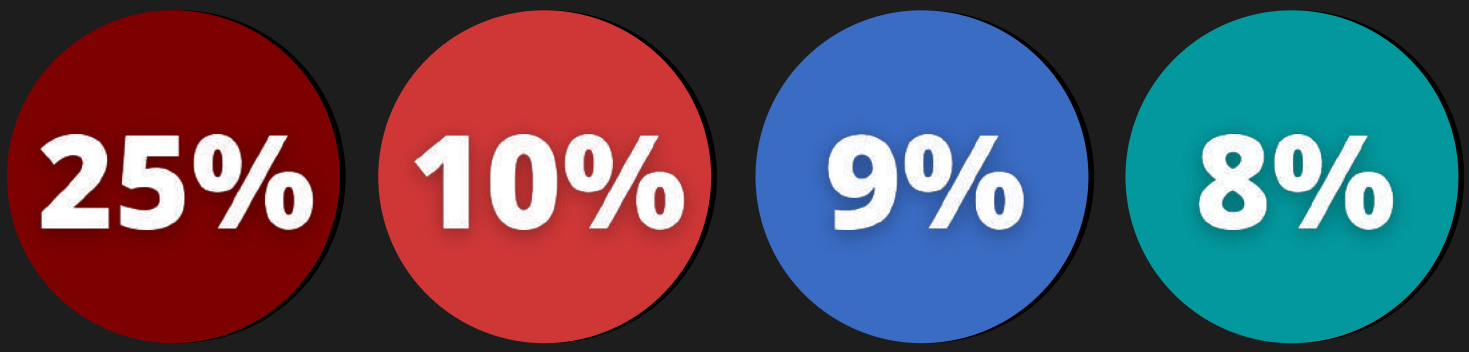
MAZE

- 21% Indústria/ Manufatura
- 10% Engenharia/ Arquitetura
- 9% Tecnologia
- 9% Saúde

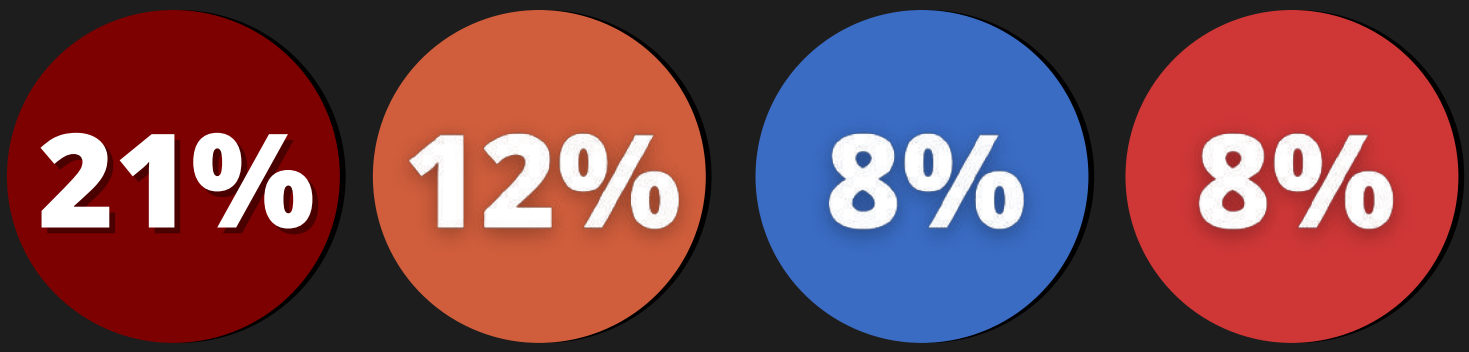
SODINOKIBI (REVIL)

- 18% Indústria/ Manufatura
- 11% Outros
- 10% Advocacia
- 10% Tecnologia

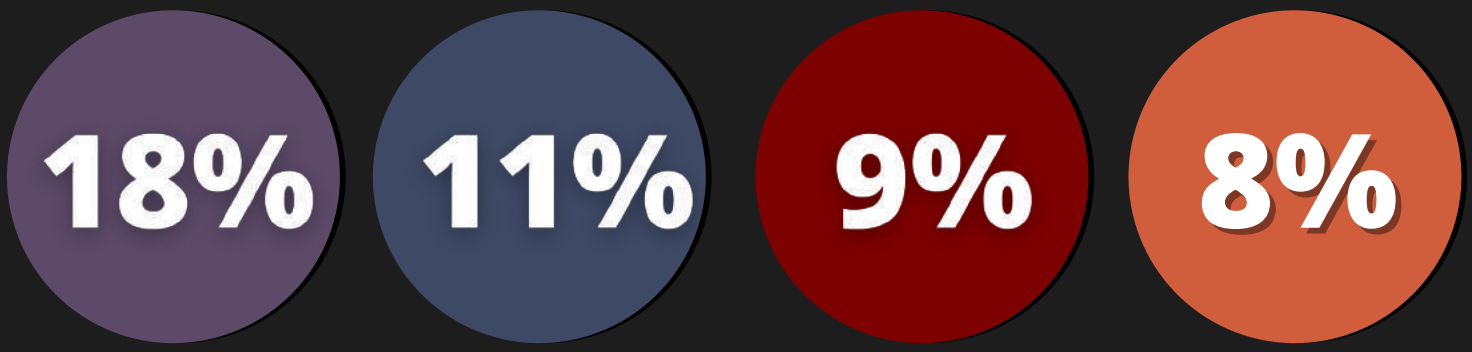
EGREGOR



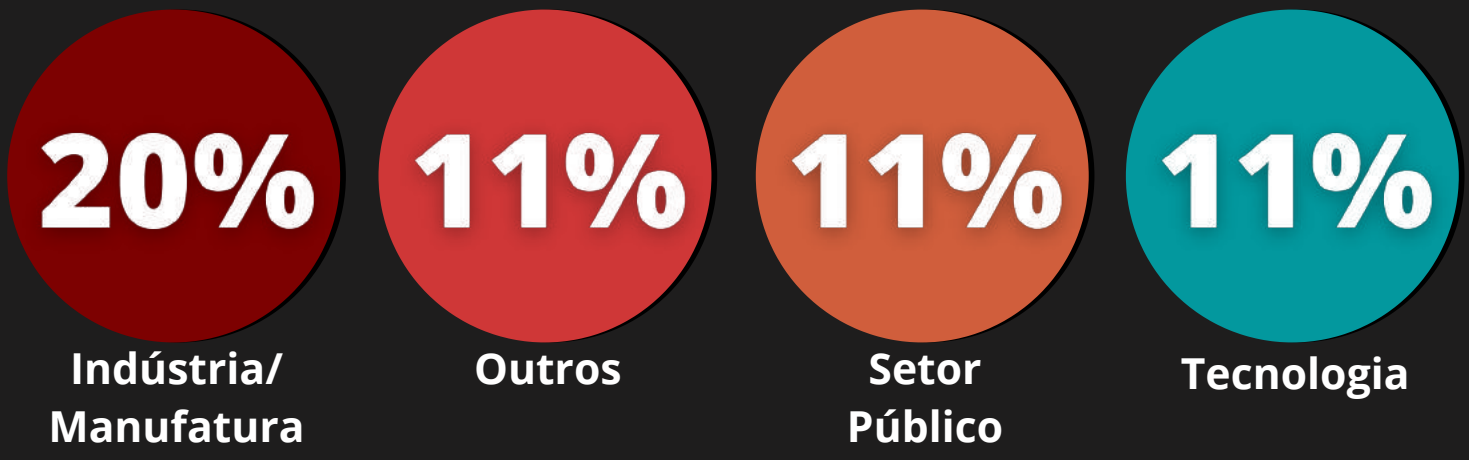
DOPPELPAYMER



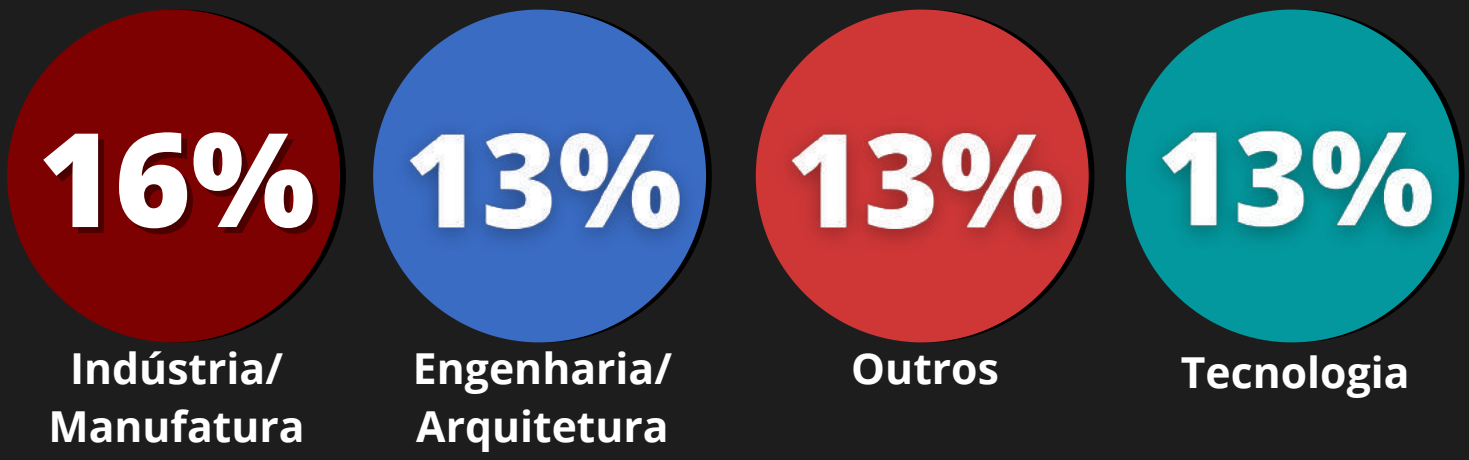
PYSA



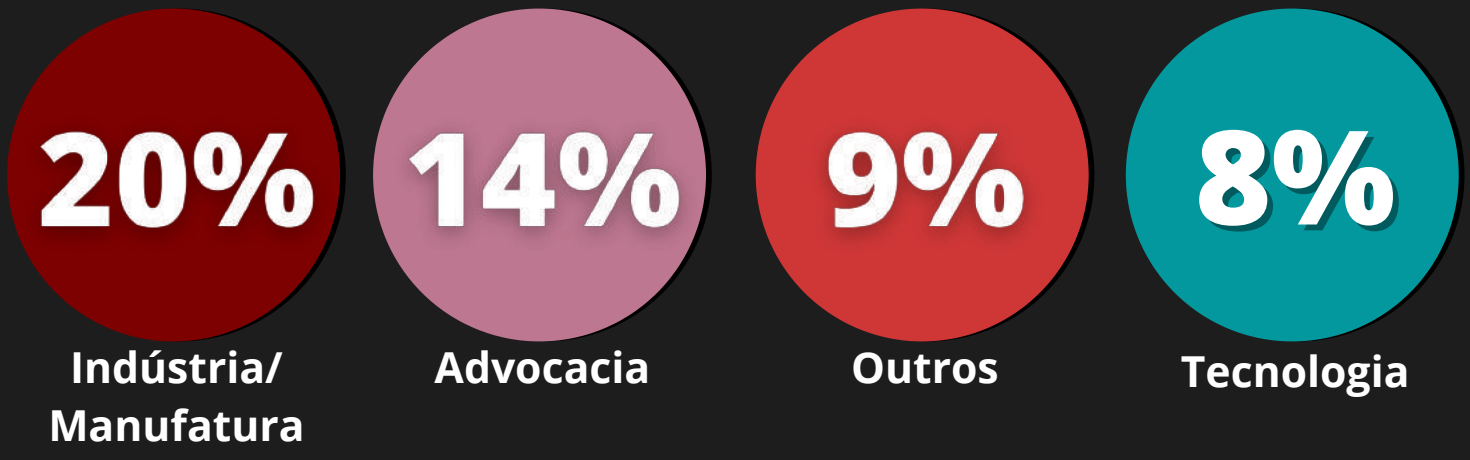
AVADDON



NETWALKER



DARKSIDE



NO BRASIL: 69 EMPRESAS

Saúde	12
Indústria/Manufatura	11
Setor Público	7
Finanças	6
Outros	6
Transporte/Logística	5
Energia	5
Engenharia/Arquitetura	4
Alimentos/Bebidas	3
Varejo/Atacado	3
Combustível	2
Tecnologia	2
Advocacia	2
Moda	1

O Brasil é um dos países do mundo com mais publicações de empresas vítimas de ransomware em sites da Dark Web, ocupando a sétima colocação entre os mais visados. Empresas da área da saúde foram as que tiveram mais informações publicadas, seguidas de empresas do ramo industrial/manufatureiro.

Dos 39 grupos de ransomware identificados publicando informações das vítimas em sites da Dark Web, 16 foram responsáveis por divulgar dados de empresas brasileiras.

MAZE	10
Avaddon	9
Prometheus	9
Pysa	7
Egregor	7
Conti	6
Nefilim	5
DarkSide	4
RansomEXX	3
Sodinokibi (REvil)	3
Sekhmet	1
NetWalker	1
Ragnar_Locker	1
Mount Locker	1
Ragnarock	1
Everest	1

NÚMERO DE VÍTIMAS DE RANSOMWARE POR ÁREA DE ATUAÇÃO NO BRASIL

SAÚDE

CONTI 3 | MAZE 2 | PYSA 2 | PROMETHEUS 2

SODINOKIBI (REVIL) 1 | NEFILIM 1 | AVADDON 1

INDÚSTRIA/MANUFATURA

EGREGOR 4 | MAZE 2 | RANSOMEXX 1

SODINOKIBI (REVIL) 1 | PROMETHEUS 1

PYSA 1 | DARKSIDE 1

SETOR PÚBLICO

AVADDON 4 | MAZE 1 | PYSA 1 | EVEREST 1

FINANÇAS

MAZE 1 | NEFILIM 1 | PYSA 1 | EGREGOR 1

RANSOMEXX 1 | PROMETHEUS 1

OUTROS

PROMETHEUS 3 | CONTI 2 | DARKSIDE 1

TRANSPORTE/LOGÍSTICA

EGREGOR 2 | MAZE 1 | SEKHMET 1

PROMETHEUS 1

ENERGIA

DARKSIDE 2 | MAZE 1 | NETWALKER 1 | RAGNAR_LOCKER 1

ENGENHARIA/ARQUITETURA

PYSA 1 | MAZE 1 | MOUNT LOCKER 1 | NEFILIM 1

ALIMENTOS/BEBIDAS

MAZE 1 | AVADDON 1 | CONTI 1

VAREJO/ATACADO

NEFILIM 1 | AVADDON 1 | RAGNAROCK 1

COMBUSTÍVEL

NEFILIM 1 | RANSOMEXX 1

ADVOCACIA

AVADDON 1 | SODINOKIBI (REVIL) 1

TECNOLOGIA

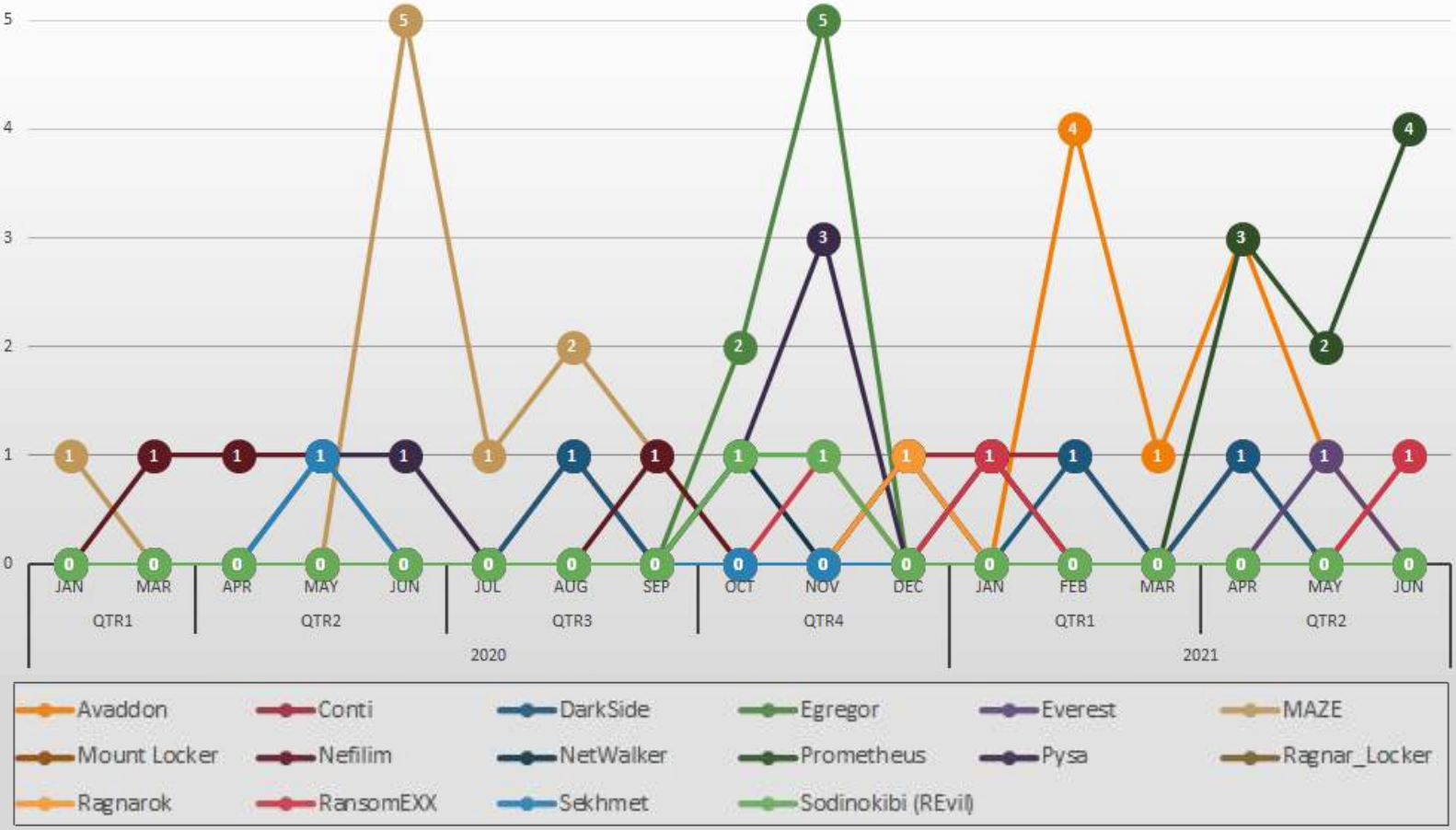
PYSA 1 | AVADDON 1

MODA

PROMETHEUS 1

EVOLUÇÃO DAS PUBLICAÇÕES DE ATAQUES DE RANSOMWARE A EMPRESAS BRASILEIRAS

(DE JANEIRO/2020 A JUNHO/2021)



Este gráfico permite ver como algumas amostras de ransomware surgem, alcançam o ápice de atividade e depois desaparecem, para dar lugar a outra amostra.

Os analistas de segurança da informação sugerem que, normalmente, quando algum grupo por detrás de um ransomware afirma estar encerrando as atividades, na verdade, está apenas mudando de nome e de amostra para poder evitar serem facilmente detectados e responsabilizados pelos ataques já realizados anteriormente.

DISTRIBUIÇÃO GEOGRÁFICA DAS EMPRESAS VÍTIMAS DE PUBLICAÇÕES EM SITES DA DARK WEB

O mapa mostra como as empresas vítimas dos ransomwares que tiveram dados publicados na Dark Web estão espalhados por todo o mundo. Estão presentes em todos continentes.

Os Estados Unidos aparecem como o país mais atingido. Não causa surpresa, tendo em vista que é a maior economia do mundo, o que os torna um alvo bastante atrativo para os operadores de ransomware e seus afiliados.

Por outro lado, a Rússia foi um dos poucos países, e o único entre as maiores potências mundiais, que não teve dado de nenhuma empresa publicado na Dark Web.

Ainda que a maioria dos grupos de ransomware em atividade afirme ter como objetivo apenas o ganho financeiro, esse panorama permite questionar se algum componente ideológico também não esteja presente nos ataques.

PRINCIPAIS ACHADOS

- O ramo de atividade que teve mais informações divulgadas na Dark Web em todo o mundo foi o de Indústria/Manufatura.
- O grupo de ransomware que mais publicou informações de empresas em site da Dark Web foi o Conti.
- Os Estados Unidos foram o país cujas empresas figuraram mais vezes nas publicações dos grupos de ransomware na Dark Web.
- O Brasil foi o sétimo país no mundo com mais empresas tendo dados publicados na Dark Web.
- Das nações mais ricas do mundo, a Rússia foi a única que não teve nenhum dado divulgado pelos grupos de ransomware na Dark Web.
- O grupo de ransomware que publicou mais informações sobre empresas brasileiras na Dark Web foi o MAZE.
- No Brasil, empresas da área da saúde foram as que tiveram mais informações divulgadas na Dark Web.
- Enquanto MAZE e Egregor foram os grupos de ransomware que mais publicaram informações de empresas brasileiras em 2020, Prometheus e Avaddon tem sido os mais ativos em 2021, até 30 de junho.
- Das 1014 amostras de ransomware que estima-se que existam ou tenham existido, apenas uma parcela muito pequena (39) foi identificada publicando informações das empresas vitimadas, menos de 4% do total.
- Dá-se muito destaque às empresas atingidas por ransomware, mas muitos grupos atacam também indivíduos, o que faz com o que número real de vítimas dessa ameaça em todo o mundo seja praticamente impossível de estimar.

CONSIDERAÇÕES FINAIS

Os Ransomwares (ou a ideia por detrás deles) não são uma ameaça recente e não se deve esperar que desapareçam tão cedo. Grupos como MAZE, Avaddon, Egregor, Darkside, mais recentemente o REvil, anunciam publicamente a suspensão das atividades maliciosas e logo são substituídos por outro. Às vezes são os mesmos atores, recomeçando sob um novo nome e utilizando uma nova amostra.

O faturamento de alguns desses grupos pode ultrapassar dezenas de milhões de dólares, e o custo de operação é proporcionalmente muito baixo. A tática de usar afiliados para executarem os ataques, enquanto os operadores se mantêm escondidos por detrás da cortina garantem uma certa segurança contra a ação das forças da lei, assim como a possibilidade de os ataques serem executados a partir de qualquer lugar do mundo e a cobrança dos valores em criptomoedas. Sob essas condições, o negócio de Ransomware se torna extremamente atrativo para os criminosos.

Não é coincidência que o ramo mais visado pelos grupos seja o industrial. O prejuízo a que uma indústria se submete ao ter seus sistemas produtivos interrompidos por um ataque de Ransomware justifica, do ponto de vista financeiro, o pagamento das quantias exigidas pelos atores de ameaça.

Do ponto de vista ético e legal, a discussão é mais complexa. Pagar os resgates alimenta o negócio das gangues de Ransomware, dá a elas mais recursos. Um grupo bem-sucedido financeiramente angaria mais afiliados, o que gera ainda mais ataques. Vários países, entre eles o mais afetado pelos ataques, os EUA, estudam a possibilidade de penalizar o pagamento dos resgates na tentativa de desestimular esse mercado cibercriminoso.

Ataques como o que interrompeu a distribuição de combustíveis pela Colonial Pipeline, gerando um aumento de preço da gasolina, corrida desenfreada da população para comprar combustível e desabastecimento nos postos, fizeram com que os EUA equiparassem, em termos de disponibilização de recursos investigativos, os ataques de Ransomware a atividades terroristas. Tal é a gravidade da ameaça.

Os cibercriminosos estão sempre atualizando o modus operandi. Buscam novas vulnerabilidades para explorar a fim de obter acesso aos sistemas das vítimas. O mercado de credenciais roubadas e de venda de acessos remotos está mais aquecido do que nunca. Envios de phishing em massa, aluguel de servidores para hospedagem dos malwares, até mesmo contratar programadores experientes para aperfeiçoarem o código dos Ransomware, nada disso está fora do alcance dos recursos financeiros desses atores. Todo gasto para eles é investimento.

Então, o que fazer? Preparar-se. E estar preparado implica na mesma atitude: investimento. É preciso investir em sistemas de segurança eficientes, backups frequentes, treinamento de equipes, atualização dos sistemas, protocolos de troca de senhas constantes, e, talvez o mais importante, informação. Informação atual, útil e acionável pode ser a diferença entre estar um passo à frente ou vários passos atrás dos adversários.

A Apura Cyber Intelligence é uma empresa brasileira especializada em Threat Intel, Segurança Cibernética e Investigação em Meios Digitais. Possuímos desenvolvimento próprio de produtos, serviços gerenciados em segurança da informação e know-how para a implementação de projetos complexos.

apura

www.apura.com.br
info@apura.com.br
linkedin.com/company/apura
facebook.com/apura.oficial
twitter.com/apura_oficial

SÃO PAULO
(11) 5504-1966

BRASÍLIA
(61) 3255-1245