Relatório de inteligência de detecção de ameaças

Cenário das ameaças de 2020

Veja o que escapou do perímetro

VMware Threat Analysis Unit

vmware®

Relatório de inteligência de detecção de ameaças

Cenário das ameaças de 2020

Resumo executivo

As violações de segurança são uma realidade hoje em dia. Os invasores sofisticados são numerosos e determinados demais para serem pegos pelas defesas do perímetro. É relativamente fácil tirar proveito das vulnerabilidades na borda da rede ou enganar um usuário para que ele conceda acesso ao dispositivo que está utilizando. A partir daí, os invasores podem esperar por dias, semanas ou meses até o momento certo para se espalhar para outros sistemas mais críticos, oferecer uma carga útil mal-intencionada e executar o objetivo, seja ele qual for. A questão não é se o ataque será bem-sucedido, e sim quando será. As organizações se beneficiam de uma equipe de segurança que muda o foco da prevenção contra todos os ataques para a interrupção da propagação de ataques após a violação inicial.

Os dados confirmam isso.

O relatório a seguir da VMware Threat Analysis Unit é um resumo dos principais dados e descobertas de julho a dezembro de 2020. Ele destaca as ameaças que escaparam das defesas do perímetro e foram identificadas por sensores da VMware colocados dentro do perímetro.

As descobertas são claras: apesar de uma estrutura de defesas implantada, agentes mal-intencionados estão operando ativamente na rede. A pesquisa mostra um retrato nítido de como os invasores evitam a detecção no perímetro, infectam sistemas e tentam se espalhar lateralmente pela rede para executar o objetivo. Armados com esse conhecimento, os diretores de segurança da informação (CISOs, pela sigla em inglês) e as equipes de segurança de rede podem ter informações essenciais sobre como combater essas ameaças, interromper a disseminação delas e ajudar a evitar que elas causem danos reais quando estiverem dentro da rede.

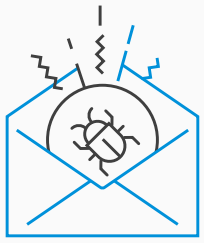
A análise inclui

Telemetria de elementos do NSX Advanced Threat Analyzer, uma sandbox de rede que oferece um ambiente exclusivo de isolamento e inspeção de malwares que emula todo o host

Telemetria de rede do NSX Advanced Threat Prevention, que inclui análise de tráfego de rede e prevenção e detecção de intrusões

Análise adicional profunda de ameaças de ataques reais executados na segunda metade de 2020

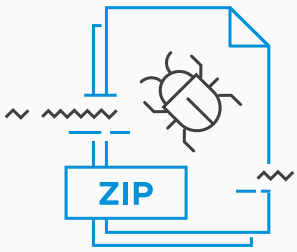
Principais informações



OS E-MAILS CONTINUAM SENDO USADOS COMO O VETOR DE ATAQUE MAIS COMUM PARA CONSEGUIR ACESSO INICIAL: MAIS DE 4% DE TODOS OS E-MAILS COMERCIAIS ANALISADOS CONTÊM UM COMPONENTE MAL-INTENCIONADO

Informações

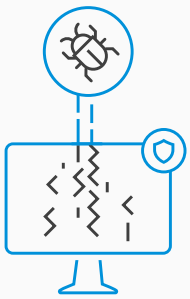
Os autores de e-mails mal-intencionados são inteligentes e incessantes. Eles estão constantemente desenvolvendo novas e diferentes maneiras de nos enganar e atacar. Embora as cargas úteis mal-intencionadas encontradas em ataques realizados por e-mail mudem frequentemente, a grande maioria dos criminosos cibernéticos usa principalmente três estratégias básicas: anexos mal-intencionados, links para páginas da Web mal-intencionadas e estratégias para realizar transações. As soluções de segurança de perímetro, como ferramentas antivírus, antimalware e antiphishing, são ineficazes contra ameaças avançadas realizadas por e-mail, e os agentes mal-intencionados continuarão usando esse meio como vetor de ataque.



MAIS DA METADE DE TODOS OS ELEMENTOS MAL-INTENCIONADOS ANALISADOS FORAM DISTRIBUÍDOS EM UM ARQUIVO ZIP

Informações

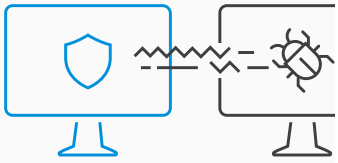
Os invasores aumentaram muito as operações por meio de campanhas de e-mail, transformando os anexos de arquivos ZIP em uma arma com conteúdo mal-intencionado. Os invasores estão bem cientes do fato de que as ferramentas de sandbox tradicionais também não conseguem analisar arquivos raros e obscuros, tornando essas ferramentas ineficazes para a detecção de ameaças. Muitas soluções de segurança tratam os arquivos ZIP protegidos por senha como arquivos criptografados e ignoram a inspeção. Uma ferramenta de sandbox mais moderna é necessária para identificar essas ameaças e examinar o maior número possível de tipos de arquivo.



A EVASÃO DA DEFESA É A TÁTICA MITRE ATT&CK® MAIS ENCONTRADA USADA POR MALWARES, SEGUIDA DA EXECUÇÃO E DA DETECÇÃO

Informações

A primeira tarefa das fontes de ameaças é evitar a detecção. Depois disso, é essencial que elas se tornem persistentes em um ambiente, o que é feito com a execução de elementos mal-intencionados. Uma vez que as ameaças tenham se tornado persistentes, começa a detecção de processos do sistema e de ativos de rede. Quando os invasores comprometem um ativo em uma rede, esse dispositivo geralmente não é o destino final. Todas essas táticas ocorreram por trás do firewall, o que significa que essas ameaças já escaparam dos controles de segurança de perímetro.

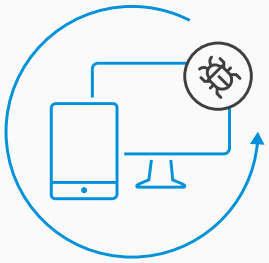


MAIS DA METADE DAS IRREGULARIDADES DE REDE DETECTADAS SÃO BEACONS INCOMUNS, SEGUIDAS DE CONEXÕES EM PORTAS SUSPEITAS E CONEXÕES ANÔMALAS ENTRE DOIS HOSTS

Informações

Beacons incomuns são evidências incontestáveis de invasão e emitem constantemente um sinal para o destino pretendido. A maioria das comunicações com um beacon acontece "às claras"; elas não são criptografadas, e os invasores estão cada vez mais usando-as como um gateway dentro do data center de uma organização. Identificar e sinalizar beacons irregulares é um método eficaz de detecção e prevenção de ameaças que pode ser realizado por uma equipe de segurança empresarial.

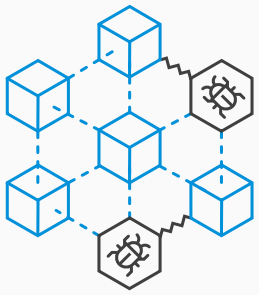
Principais informações



MAIS DE 60% DE TODOS OS EVENTOS DE SEGURANÇA DE COMANDO E CONTROLE ESTÃO RELACIONADOS A UM APLICATIVO COMERCIAL DE CONTROLE REMOTO

Informações

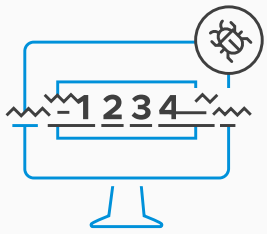
As fontes de ameaças transformaram em arte a atividade de se esconder bem. O uso de ferramentas de gerenciamento comuns para se comunicar com o invasor permite que ele disfarce as transmissões junto com o tráfego legítimo. O problema é que, quando você elimina um malware, ele se conecta tanto a sites perigosos quanto a endereços seguros. Ele realiza muitas atividades que não têm nada a ver com o tráfego mal-intencionado nem com a atividade de comando e controle, exploração ou extração. Por exemplo, ele pode se conectar a um site conhecido para verificar a conectividade com a Internet ou se conectar a servidores de e-mail legítimos para enviar spam. Se você classificar cada destino de tráfego como mal-intencionado, poluirá bastante os conjuntos de treinamento. Para identificar com precisão a atividade das ameaças e entender quais atividades são conexões de comando e controle, quais são conexões de movimento lateral, quais são exploits e o que é ruído, são necessários algoritmos de aprendizado de máquina (ML, pela sigla em inglês) treinados.



NA REDE EMPRESARIAL, OS EVENTOS ASSOCIADOS À ATIVIDADE DE MINERAÇÃO DE CRIPTOMOEDAS REPRESENTAM UM QUARTO DE TODAS AS AMEAÇAS CONHECIDAS

Informações

Certamente há riscos potenciais em ter a rede comprometida por um malware de mineração de criptomoedas. Não são apenas dados ou a propriedade intelectual que estão em jogo. Muitas ameaças de segurança exploram recursos de rede para fins mal-intencionados. Os criminosos podem, para usar uma frase do jargão de vendas empresariais, "aterrissar e expandir", o que significa ter um conjunto inicial de malwares instalado e o canal de comando e controle em operação. Depois, é feito o download de um malware mais agressivo. Eles também podem vender os sistemas comprometidos para outros criminosos, com outras intenções.



A PRÁTICA DE SEGURANÇA INADEQUADA MAIS COMUM DETECTADA É O USO DE SENHAS EM TEXTO SIMPLES

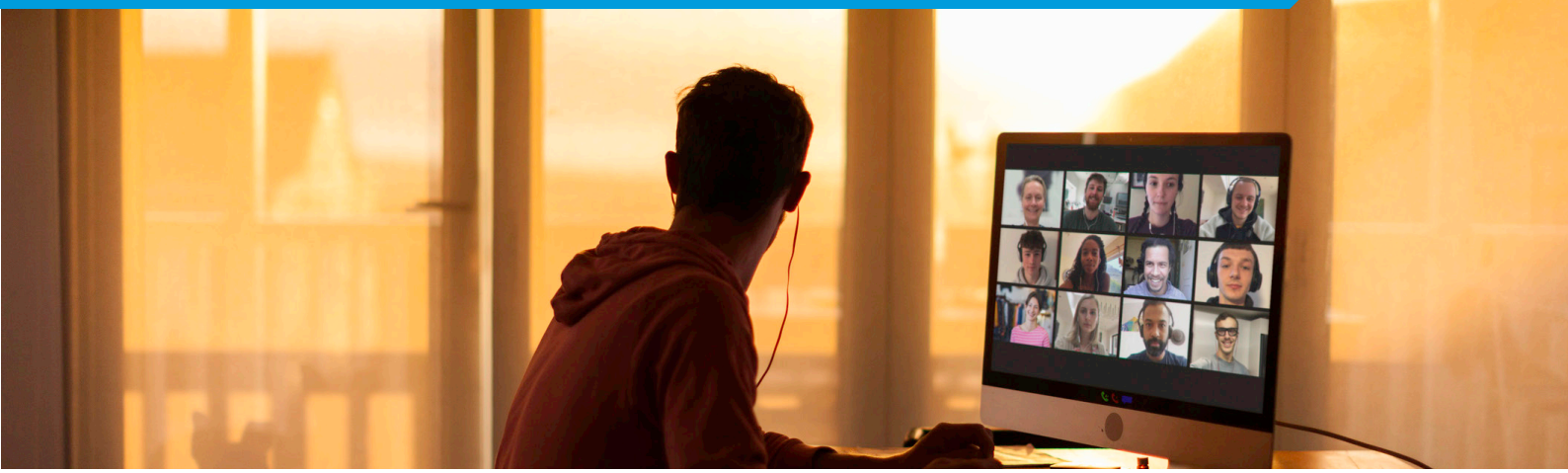
Informações

Esses eventos de segurança são facilmente evitáveis. A transmissão pela rede de senhas em texto simples podem ser a porta de entrada dos invasores, permitindo que eles se movam lateralmente e extraiam dados.

MAIS DE 75% DOS EVENTOS DE MOVIMENTAÇÃO LATERAL IDENTIFICADOS FORAM REALIZADOS COM O USO DO REMOTE DESKTOP PROTOCOL (RDP), MUITAS VEZES USANDO CREDENCIAIS ROUBADAS PARA FAZER LOGIN EM OUTROS HOSTS NA REDE

Informações

Embora existam várias maneiras diferentes de se propagar lateralmente, o registro em log em hosts via RDP usando senhas em texto simples e expostas pela rede (veja as estatísticas acima), contas válidas ou credenciais obtidas com métodos de força bruta ainda é a técnica mais comum. Quando os invasores comprometem um ativo em uma rede, esse dispositivo geralmente não é o destino final. Para atingir o objetivo, é provável que os malfeitores invadam um servidor da Web, o dispositivo de endpoint de um funcionário ou algum outro local. Depois, eles se movem lateralmente pela rede a partir desse comprometimento inicial do dispositivo para alcançar o destino desejado. O comprometimento inicial raramente causa danos graves. Se as equipes de segurança conseguirem detectar a movimentação lateral antes que os invasores atinjam os destinos desejados, elas poderão impedir o acesso a dados confidenciais. As equipes de segurança empresarial podem usar inteligência artificial (AI, pela sigla em inglês) e ML para determinar conexões RDP anormais.



Introdução

2020 mudou de maneiras inimagináveis o modo como as pessoas trabalham. A pandemia global de COVID-19 e o impacto econômico que ela causou afastaram os usuários da proteção e da segurança oferecidas pelas defesas do perímetro. Muitas pessoas começaram a trabalhar em casa, acessando sistemas de negócios essenciais por meio de conexões VPN ou diretamente com plataformas de software como serviço (SaaS, pela sigla em inglês) e outros aplicativos em nuvem.

As fontes de ameaças imediatamente se aproveitaram da situação, usando a ansiedade pandêmica como um gatilho para ataques de engenharia social. Esses ataques se concentraram cada vez mais em ransomware, buscando especialmente vítimas de alta visibilidade. Além disso, estamos passando por um ressurgimento de exploits desatualizados, provavelmente visando a computadores sem manutenção recorrente.

O problema principal causado por esses hosts comprometidos, mesmo que não estejam fisicamente nas instalações de uma organização, é que eles podem conceder acesso a contas e hosts com privilégios maiores em redes empresariais, bem como em data centers empresariais. Em alguns incidentes, os invasores estão usando dispositivos de usuários previamente comprometidos para conseguir acesso aos controladores de domínio do Windows, que são utilizadoscomo um mecanismo extremamente eficaz para a distribuição de componentes de ransomware pela rede. Além disso, a pandemia impulsionou o uso da infraestrutura de desktop virtual (VDI, pela sigla em inglês), do RDP e do desktop como serviço (DaaS, pela sigla em inglês), criando uma combinação de tráfego de aplicativos e usuários no data center.

Por conta dessas mudanças, é fundamental que as equipes de segurança empresarial ampliem os recursos de detecção e prevenção de ameaças além do firewall para cobrir todo o tráfego leste-oeste.

As informações a seguir foram extraídas de dados coletados de julho a dezembro de 2020 por sensores da VMware implantados em uma ampla variedade de redes empresariais. Essas redes são grandes e pequenas e cobrem diversos setores da indústria. Os sensores da VMware são quase sempre implantados atrás de firewalls de perímetro e no data center, fornecendo informações exclusivas sobre os ataques que já violaram as defesas do perímetro. Esses ataques bastante evasivos, sofisticados e com objetivos muito concretos estão tentando ativamente espalhar e entregar cargas úteis mal-intencionadas para extrair dados.

Telemetria de elementos

A sandbox de rede oferece um ambiente exclusivo de isolamento e inspeção que emula todo o host, incluindo a CPU, a memória do sistema e todos os dispositivos de entrada e saída. Ela funciona por meio da interação com o malware para analisar comportamentos de maneira segura e avalia elementos de malware que escapam do perímetro e atravessam o data center. Ao longo desse período de seis meses, a oferta do Advanced Threat Prevention (ATP) na solução NSX Service-defined Firewall (SDFW) obteve informações valiosas sobre como os elementos tentavam se infiltrar nos dispositivos finais.

Existem três classes de elementos: benignos, suspeitos e mal-intencionados. Elementos benignos (por exemplo, documentos, executáveis, bibliotecas) não representam uma ameaça ativa. Elementos suspeitos são, em sua maioria, incômodos de risco baixo, mas não devem ser desconsiderados, pois a natureza deles pode mudar rapidamente (ou com uma atualização). Elementos mal-intencionados são os componentes mais agressivos e destrutivos, geralmente distribuídos por meio de um processo de várias etapas cujo objetivo é confundir os sistemas de detecção e ocultar ações mal-intencionadas entre os diversos eventos da rede.

A porcentagem de ocorrência dessas classes de elementos foi relativamente constante durante esse período. Como mostra a figura abaixo, a porcentagem de elementos mal-intencionados detectados é de cerca de 0,1%.

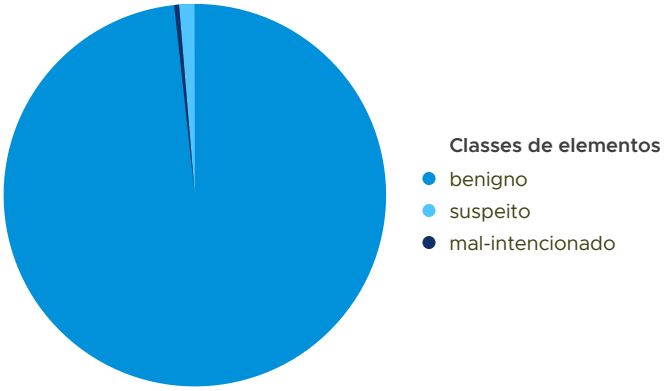


FIGURA 1: PORCENTAGENS DE ARQUIVOS BENIGNOS, SUSPEITOS E MAL-INTENCIONADOS EM TODO O PERÍODO DO RELATÓRIO.

Analisando os tipos de arquivo mais comuns observados, há uma clara diferença entre elementos benignos e mal-intencionados: enquanto os benignos são principalmente tipos de arquivo bem conhecidos e compreendidos (como arquivos PDF, mostrados na Figura 2), os elementos mal-intencionados dependem de vários tipos de arquivo obscuros mais raros, como arquivos ISO9660 e ACE (consulte a Figura 3).

O uso de tipos de arquivo incomuns para fornecer elementos mal-intencionados se deve, em parte, à tentativa de ocultar conteúdo em pacotes difíceis de analisar e, às vezes, à exploração de falhas de segurança em softwares desatualizados e sem aplicação de patches que são utilizados para gerenciar esses tipos de arquivo.

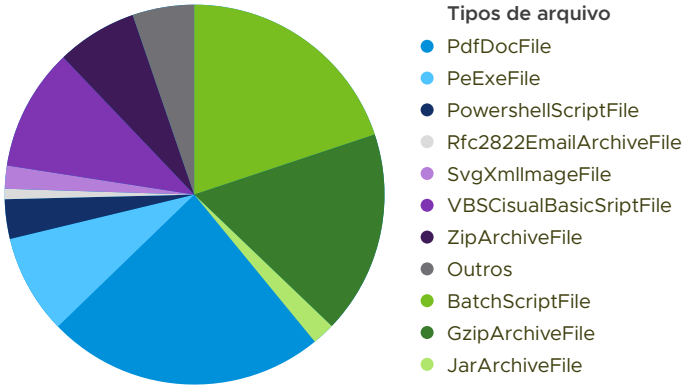


FIGURA 2: PRINCIPAIS TIPOS DE ARQUIVO OBSERVADOS EM ELEMENTOS BENIGNOS.

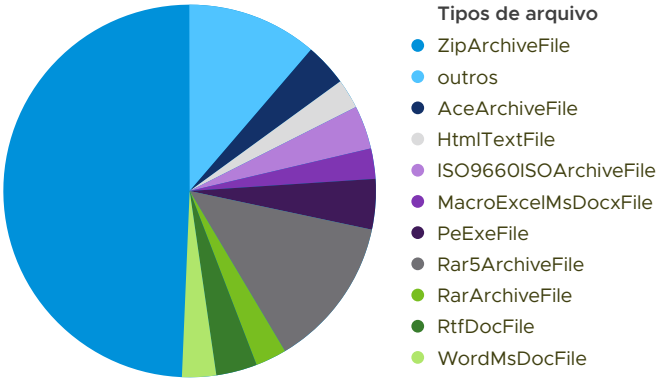


FIGURA 3: TIPOS DE ARQUIVO MAIS COMUNS EM ELEMENTOS MAL-INTENCIONADOS.

O gráfico da Figura 4 mostra a porcentagem de elementos mal-intencionados observados durante o período analisado. Ao longo de todo o período, a porcentagem observada de elementos mal-intencionados é inferior a 0,5%, exceto por dois picos que ocorreram durante os meses de junho e novembro. O primeiro pico (em junho) representa uma campanha de spams mal-intencionados que distribuiu o ransomware Avaddon. A fonte de ameaças usou arquivos ZIP que continham arquivos JavaScript mal-intencionados. Esses elementos iniciam um comando do PowerShell que recupera e executa a carga útil do ransomware. O segundo pico (em novembro) foi causado por uma campanha de spams mal-intencionados realizada pelo botnet Phorpiex. A fonte de ameaças distribuiu arquivos ZIP que continham executáveis mal-intencionados que faziam download do malware BitRansomware e o executavam [1].

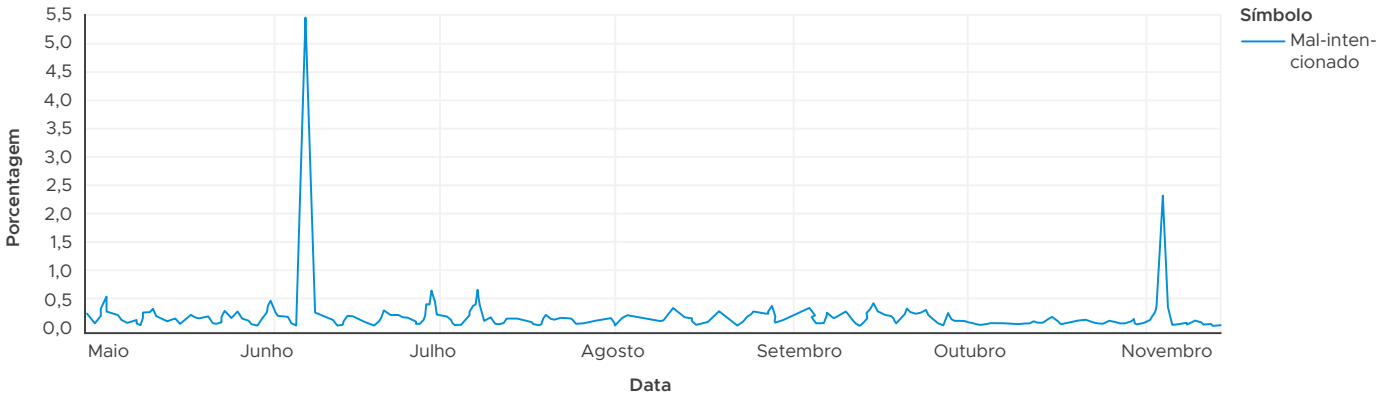


FIGURA 4: PORCENTAGEM DE ELEMENTOS MAL-INTENCIONADOS OBSERVADOS DURANTE O PERÍODO.

Para entender melhor como os invasores tiram proveito de vários vetores de distribuição, analisamos as taxas de identificação de arquivos mal-intencionados e suspeitos para cada vetor com base nos dados de telemetria gerados por organizações nos EUA e na região EMEA durante todo o período, conforme mostrado na Figura 5. Os dados mostram que o vetor mais comum utilizado para malware é o e-mail, que tem uma taxa de identificação de quase 4%. Isso não é surpreendente. O e-mail ainda é o mecanismo de comunicação mais comum nas organizações e, por isso, pode causar taxas de infecção maiores em comparação com outros vetores. Por outro lado, o SMB exibe a maior taxa de identificação de arquivos suspeitos em todos os vetores, com mais de 3% de todos os arquivos transferidos pelo protocolo marcados como suspeitos. A investigação mostra que a maioria desses arquivos é composta de ferramentas de gerenciamento de TI, como scripts de lote que são compartilhados via SMB pela equipe de TI para atualizações do Windows. Antigamente, as fontes de ameaças usavam ambos os tipos de arquivo para espalhar malwares. Por isso, esses tipos são marcados como suspeitos.

Com essa introdução em mente, as ameaças feitas por meio dos vetores identificados a seguir foram detectadas atrás do firewall do perímetro. A implantação de uma sandbox de rede para inspecionar elementos além dos controles do perímetro provavelmente reduziria as taxas de infecção.

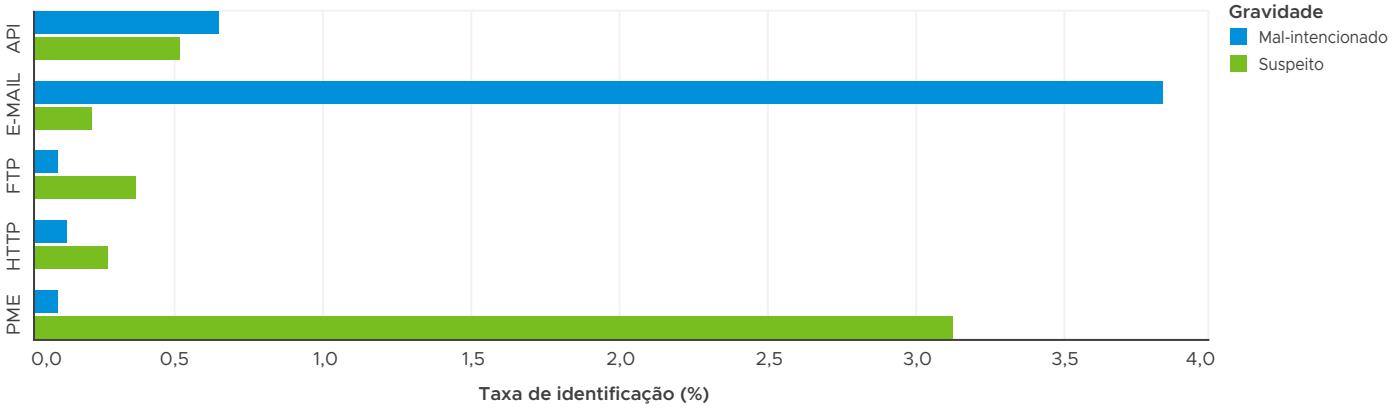
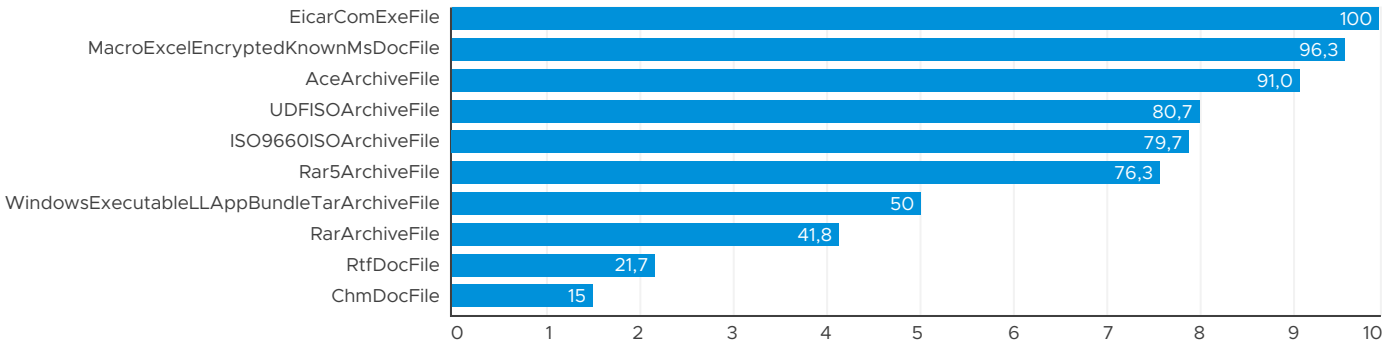


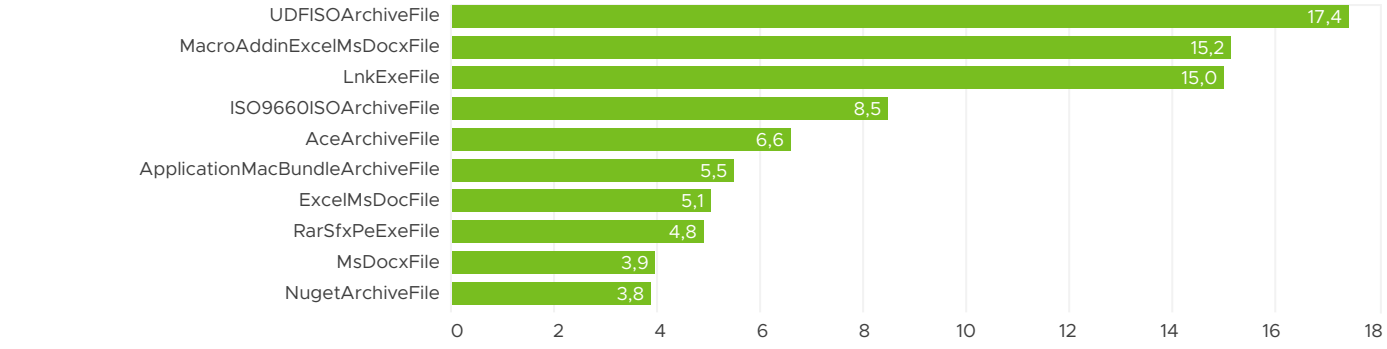
FIGURA 5: PORCENTAGENS DE ARQUIVOS MAL-INTENCIONADOS E SUSPEITOS POR VETOR DE ENTREGA EM TODO O PERÍODO.

A taxa geral de identificação de todos os tipos de arquivo foi de cerca de 1,3% durante esse período. O gráfico inferior da Figura 6 lista os principais tipos de arquivo com as maiores taxas de identificação. O primeiro lugar é ocupado pelo tipo de arquivo Universal Disk Format (UDF, denominado UDFISOArchiveFile no gráfico), que teve uma taxa de identificação de 17,4%. É importante notar que esse tipo tem a quarta maior taxa de identificação de arquivos mal-intencionados, conforme mostrado no gráfico superior. Por conta disso, não é surpreendente ver que a taxa de identificação de arquivos suspeitos é alta. Da mesma forma, outros tipos de arquivos listados no gráfico de cima também aparecem no gráfico de baixo. O tipo de arquivo MacroAddinExcelsDocxFile vem em segundo lugar no gráfico, com uma taxa de identificação de 15,2%. Os invasores são conhecidos por aproveitar bastante macros mal-intencionadas incorporadas em arquivos do Microsoft Excel para espalhar malware, como a campanha Emotet relatada no fim de 2020 [3]. Por outro lado, as macros são amplamente utilizadas para aplicativos legítimos. Com frequência, essas macros exibem características semelhantes às das equivalentes mal-intencionadas, como a execução automática da macro ao abrir um arquivo do Excel e ofuscação para proteger o código VBA contra cópia e modificação. Em grande parte, isso explica a alta taxa de identificação de arquivos suspeitos.

As taxas de identificação e os tipos de arquivo para ocorrências benignas e mal-intencionadas são muito diferentes. É altamente recomendável a implantação de uma sandbox de rede para inspecionar anexos de e-mail ou a configuração de regras de e-mail para colocar MacroExcelEncryptedKnownMSDocFile e AceArchiveFiles em quarentena, dadas essas taxas de identificação.

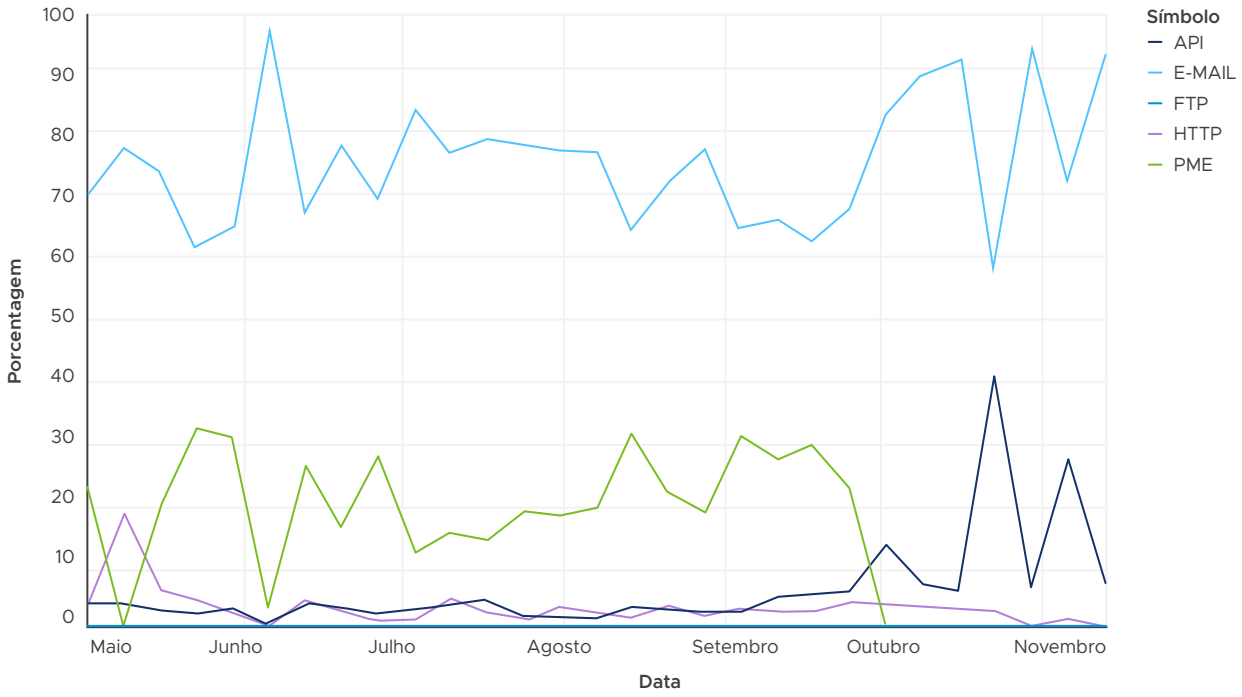


Taxa de identificação de arquivos mal-intencionados (%), com taxa geral: 0,2%



Taxa de identificação de arquivos suspeitos (%), com taxa geral: 1,3%

O gráfico a seguir, da Figura 7, mostra as tendências na linha do tempo dos elementos mal-intencionados observados por vetor de distribuição durante o período. A maioria dos elementos mal-intencionados observados na telemetria é distribuída por e-mail, o que indica que os e-mails de spear-phishing são o método mais comum utilizado pelas fontes de ameaças para enviar elementos mal-intencionados. Às vezes, os picos observados nas linhas do vetor de distribuição representam campanhas que usam esse vetor. Por exemplo, o pico observado no vetor de distribuição por e-mail durante o mês de junho representa a campanha de spams mal-intencionados que distribuiu o ransomware Avaddon.



O gráfico da Figura 8 mostra a tendência na linha do tempo da identificação de elementos mal-intencionados por tipo de arquivo. O gráfico mostra os cinco tipos de arquivo principais utilizadospelas fontes de ameaças para distribuir elementos mal-intencionados durante o período observado. A telemetria mostra que, durante a análise, a maior parte dos elementos mal-intencionados foi distribuída na forma de arquivos ZIP, que eram os arquivos usadosnos anexos de várias campanhas de e-mail.

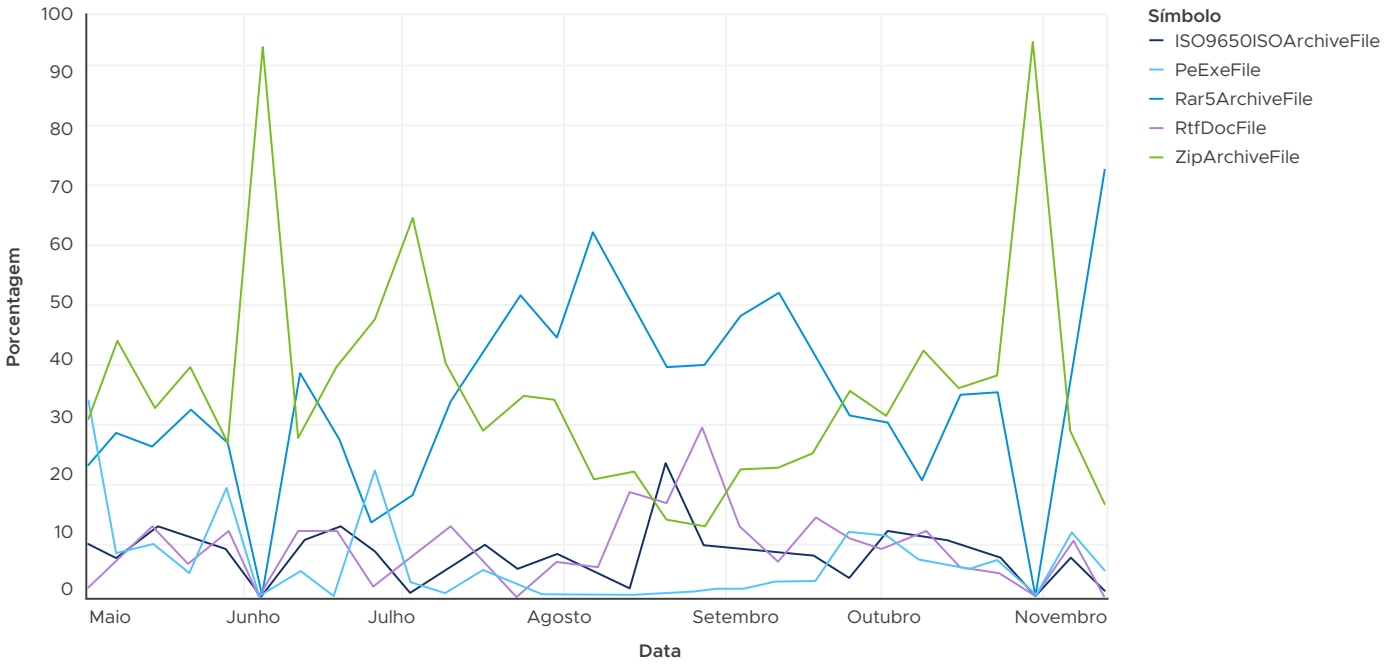


FIGURA 8: OS CINCO TIPOS DE ARQUIVOS MAL-INTENCIONADOS MAIS OBSERVADOS DURANTE O PERÍODO.

Embora os vetores de distribuição e os tipos de arquivo sejam importantes durante a avaliação do risco associado a elementos específicos, também é interessante observar o comportamento associado a elementos e ataques.

As Figuras 9 e 10 mostram as principais táticas e técnicas MITRE ATT&CK® usadas durante o período. Como mostra a Figura 9, TA0005: A evasão da defesa é a tática mais encontrada usada por malwares, seguida por TA0002: execução e TA0007: detecção. Na campanha Emotet que foi analisada recentemente [3], o malware exibe a maioria das táticas mostradas no gráfico. O malware tenta escapar da detecção (TA0005: evasão da defesa) gerando processos do PowerShell e modificando arquivos executáveis no diretório de sistema do Microsoft Windows da máquina da vítima. Além disso, o malware envia um arquivo executável (TA0002: execução) que enumera os processos em execução (TA0007: detecção) para executar código não confiável no processo do Microsoft Office (novamente TA0002: execução).

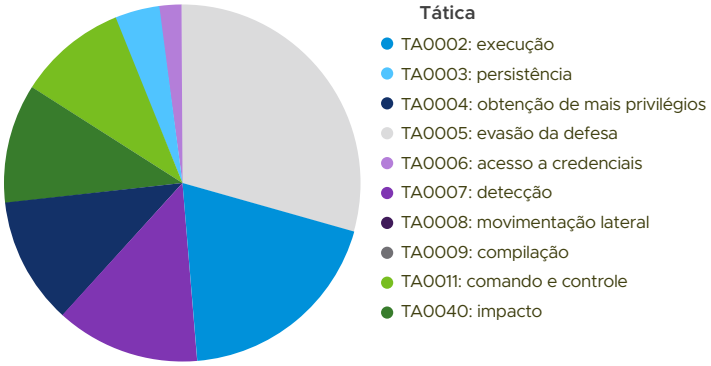


FIGURA 9: PRINCIPAIS TÁTICAS MITRE ATT&CK PARA TODO O PERÍODO.

A Figura 10 mostra as 20 técnicas principais no mesmo período. A técnica mais popular é a T1071: protocolo padrão da camada do aplicativo. Essa técnica está relacionada a atividades de rede, como fazer download de arquivos de um local remoto ou se conectar a servidores de comando e controle. Isso é muito comum em ataques que usam cargas úteis iniciais para realizar outras atividades mal-intencionadas. A segunda técnica mais comum é aproveitar a Instrumentação de Gerenciamento do Windows (WMI, pela sigla em inglês, denominada T1047: Instrumentação de Gerenciamento do Windows no gráfico) como um vetor de ataque. Os invasores podem usar a WMI para invocar processos mal-intencionados do PowerShell (T1086: PowerShell) conforme observado nos ataques Emotet [3]. De acordo com um relatório publicado em 2019 [4], quase 50% de todos os processos mal-intencionados do PowerShell foram iniciados com a WMI, e 40% foram acionados diretamente pelo cmd.exe (T1059: interface de linha de comando).

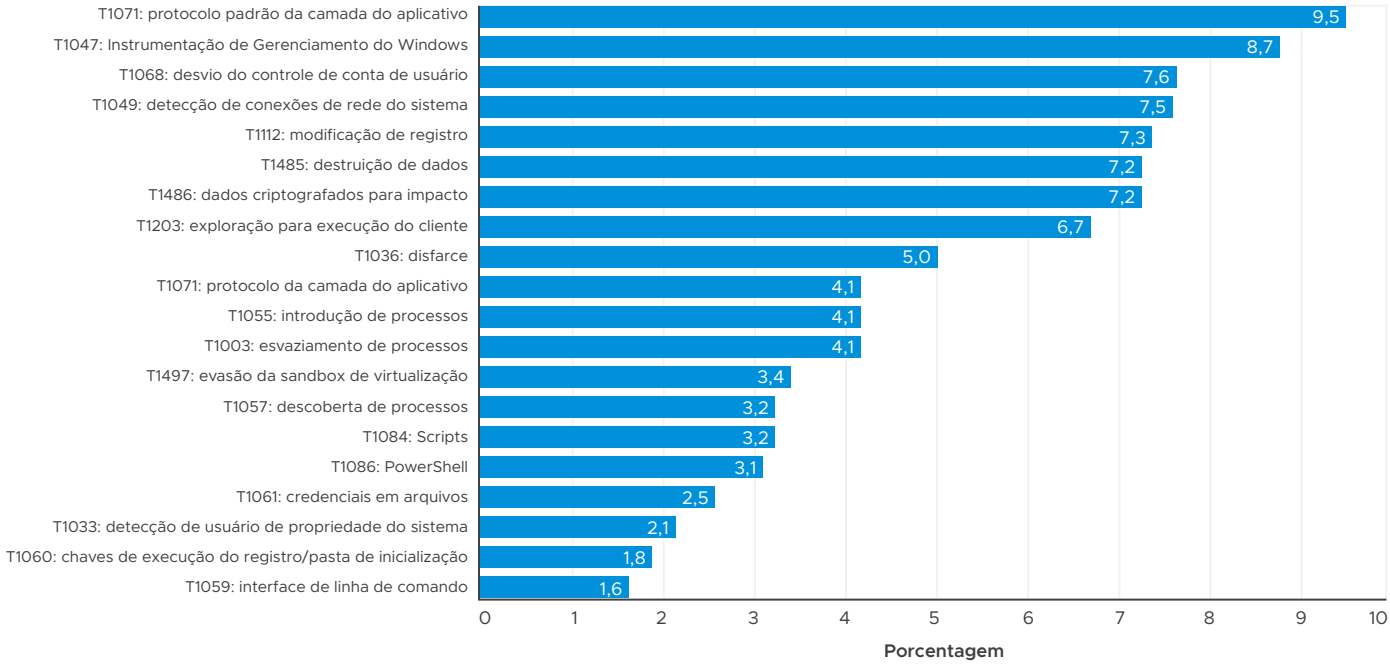


FIGURA 10: PORCENTAGEM DE OCORRÊNCIAS DAS PRINCIPAIS TÉCNICAS MITRE ATT&CK PARA TODO O PERÍODO – TOTAL DE TÉCNICAS CONSIDERADAS: 68.

Telemetria de rede

A análise da telemetria da rede nos permite compreender melhor o cenário atual de ameaças. A oferta do ATP dentro do NSX Service-defined Firewall (SDFW) tem um amplo conjunto de recursos de detecção que abrangem um IDS/IPS totalmente distribuído e análise de tráfego de rede baseada em comportamento que ajuda a fornecer informações de alta fidelidade sobre ameaças de rede que entram na rede ou se movem dentro dela.

Em diferentes classes de ameaças de eventos, a análise destaca os três tipos de eventos mais prevalentes para cada classe. Os dados mostram uma quantidade não mitigada de ruído de fundo na forma de beacons (legítimos ou não) e práticas de segurança inadequadas, como protocolos de rede não criptografados.

Os três principais eventos de "interação de rede irregular"

Mais de 50% de todas as irregularidades detectadas pelos sensores da VMware eram atividades incomuns de beacons (consulte a Tabela 1), o que significa que as redes empresariais monitoradas contêm uma série de dispositivos que contatam endpoints externos ou outros dispositivos regularmente (por motivos legítimos e como resultado de infecção). As conexões em portas suspeitas estão em segundo lugar, pois são a marca registrada de tentativas não autorizadas de acesso a recursos empresariais. Em terceiro lugar, estão as conexões irregulares entre dois hosts, que são eventos gerados quando, por exemplo, um host começa a acessar um serviço em um host que nunca acessou anteriormente.

IRREGULARIDADE	PORCENTAGEM
Atividade incomum de beacons	58,8%
Conexão em porta suspeita	22,9%
Conexão irregular entre dois hosts	8%
Outros	10,3%

TABELA 1
QUASE 60% DAS IRREGULARIDADES DETECTADAS NAS REDES EMPRESARIAIS SÃO ALGUMAS FORMAS DE USO DE BEACONS. NO ENTANTO, COMPREENDER QUAIS DELAS SÃO MAL-INTENCIONADAS E QUAIS SÃO BENIGNAS EXIGE UMA INTELIGÊNCIA SOFISTICADA DE DETECÇÃO DE AMEAÇAS.

As três principais ameaças de "comando e controle"

Essa classe de evento inclui todas as detecções de rede para as quais o protocolo de comunicação (ou os endpoints envolvidos) pode ser identificado como envolvido em atividades suspeitas com um grau de precisão suficiente. Conforme mostrado na Tabela 2, mais de 60% de todos os eventos estão relacionados a um aplicativo comercial de "controle remoto" utilizado com frequência por agentes mal-intencionados (como visto no primeiro semestre de 2020, inclusive por algumas campanhas temáticas da COVID-19 que dependem de macros XL4 do Excel). O segundo lugar é ocupado por uma ferramenta de teste de intrusão/exploração que também é utilizada com frequência por agentes sofisticados (TA505). Na sequência, estão os endpoints que se conectam a servidores de comando e controle para fazer download de cargas úteis adicionais.

AMEAÇA	PORCENTAGEM
Aplicativo de controle remoto comercial	65,2%
Ferramenta de teste de intrusão/exploração	15,3%
Endpoints que se conectam a servidores de comando e controle	9,1%
Outros	10,4%

TABELA 2
MUITAS FERRAMENTAS DE SEGURANÇA SÃO UTILIZADAS POR MALFEITORES E POR PESSOAS COMUNS; PORTANTO, ENTENDER O CONTEXTO DESSAS DETECÇÕES É A CHAVE PARA AVALIAR O IMPACTO DELAS NA REDE DE UMA ORGANIZAÇÃO.

As três classes principais de "ameaças conhecidas"

A Tabela 3 lista as classes de ameaças além de “comando e controle” ainda detectadas por assinaturas não probabilísticas ou por detectores que não usam ML. As três classes principais são violações em algum sentido: práticas de segurança inadequadas, violações de políticas e atividade de mineração de criptomoedas. As outras classes de ameaças (representadas por “Outros”) estão abaixo do limite de 10%.

Os mineradores de criptomoedas podem devorar os recursos da rede. De servidores a desktops, essas ameaças podem afetar a produtividade de uma organização e os custos da nuvem. Na rede empresarial, os eventos associados à atividade de mineração de criptomoedas podem ser responsáveis por um quarto de todas as ameaças.

CLASSE DE AMEAÇA	PORCENTAGEM
Mineração de criptomoedas	24,8%
Prática de segurança inadequada	20,2%
Violação de políticas	17,8%
Outros	37,2%

TABELA 3
CLASSES DE AMEAÇAS CONHECIDAS.

As três principais ameaças de “práticas de segurança inadequadas”

As práticas de segurança inadequadas mais comuns são a falta de criptografia adequada (consulte a Tabela 4). A mais prevalente é a adoção de servidores de e-mail e clientes que dependem da transmissão de senha em texto simples, seguido pelo mesmo problema com o FTP. A autenticação HTTP básica (um tipo de autenticação HTTP que depende de senhas em texto simples) é a terceira prática de segurança inadequada mais comum.

A solução mais simples é remover o uso de todas as credenciais que usam texto simples.

AMEAÇA	PORCENTAGEM
Transmissão de senha em texto simples POP3/SMTP	49,3%
Transmissão de senha em texto simples FTP	20,6%
Autenticação HTTP básica	15,7%
Outros	14,4%

TABELA 4
OS SERVIÇOS DA SUA REDE ESTÃO SEGUINDO AS PRÁTICAS RECOMENDADAS? 90% DOS EVENTOS ASSOCIADOS A PRÁTICAS INADEQUADAS ESTÃO ASSOCIADOS AO USO DE CREDENCIAIS EM TEXTO SIMPLES.

As três ameaças principais de “violações de políticas”

As violações de políticas mais comuns estão relacionadas ao protocolo BitTorrent (geralmente usado para compartilhamento de arquivos) em um ambiente empresarial ou ao carregamento de clientes de jogos. A terceira violação de políticas (DNS sobre HTTPS) pode ser um efeito colateral da ativação por padrão desse recurso por parte dos navegadores da Web nas configurações empresariais. Muitas das outras violações de políticas (na categoria “Outros” na Tabela 5) estão relacionadas ao tráfego VPN, que é usado com frequência para escapar de firewalls empresariais e acessar dados confidenciais.

Essas violações de políticas podem levar a atividades mal-intencionadas, muitas vezes afetam a produtividade e podem gerar violações de direitos autorais.

AMEAÇA	PORCENTAGEM
Cliente de jogos	35,4%
uTorrent	26,9%
DNS sobre HTTPS	13,6%
Outros	24,1%

TABELA 5
VIOLAÇÕES DE POLÍTICAS DE REDE PODEM GERAR CENTENAS DE MILHARES DE EVENTOS NA REDE EMPRESARIAL. O BITTORRENT E OS CLIENTES DE JOGOS PODEM SER RESPONSÁVEIS POR MAIS DE 50% DE TODAS AS VIOLAÇÕES DE POLÍTICAS NAS REDES EMPRESARIAIS.

As três técnicas principais de “movimentação lateral”

Embora não esteja relacionada a uma ameaça ou classe de ameaça específica, temos a seguir a análise de todos os eventos de rede conhecidos por exercer uma das táticas MITRE ATT&CK® mais impactantes no contexto de segurança de rede: TA0008, movimentação lateral. Conforme mostrado na Tabela 6, enquanto a maioria dos eventos de rede usou o RDP para fazer login em outros hosts com credenciais possivelmente roubadas, mais de 10% das detecções foram relacionadas a “Pass the Hash”, uma técnica utilizada para contornar mecanismos de autenticação padrão que exigem senha em texto simples contando com credenciais criptografadas (geralmente recuperadas pelo acesso direto à memória do sistema). Curiosamente, a exploração de serviços remotos por meio do infame exploit ETERNALBLUE ou outros baseados em SMB está no fim da lista, com meros 2%.

AMEAÇA	PORCENTAGEM
T1076: Remote Desktop Protocol	76,5%
T1075: Pass the Hash	12,7%
T1210: Exploração de serviços remotos	2%
Outros	8,8%

TABELA 6
EMBORA EXISTAM VÁRIAS FORMAS DIFERENTES DE SE PROPAGAR LATERALMENTE, FAZER LOGIN EM HOSTS VIA RDP USANDO CONTAS VÁLIDAS OU CREDENCIAIS OBTIDAS COM MÉTODOS DE FORÇA BRUTA AINDA É A TÉCNICA MAIS COMUM.

Combata ameaças de segurança evasivas com as soluções VMware

Esses comportamentos de ameaça podem ser resumidos desta forma:

O NSX SERVICE-DEFINED FIREWALL DA VMWARE COM O ADVANCED THREAT PREVENTION (ATP) PODE IMPEDIR O ACESSO INICIAL AO DETECTAR ELEMENTOS MAL-INTENCIONADOS E LINKS QUE TENTAM ENGANAR OS USUÁRIOS. OS RECURSOS DE ANÁLISE DE ARQUIVOS DE NÍVEL CORPORATIVO DA VMWARE USAM O DEEP CONTENT INSPECTION PARA DETECTAR AMEAÇAS AVANÇADAS QUE PERSISTEM, AUMENTAM OS PRIVILÉGIOS E EVITAM A DETECÇÃO. A ANÁLISE DE TRÁFEGO DE REDE USA UMA COMPREENSÃO PROFUNDA DE COMPORTAMENTOS MAL-INTENCIONADOS PARA DISCERNIR IRREGULARIDADES BENIGNAS DE MOVIMENTAÇÕES LATERAIS MAL-INTENCIONADAS, DETECÇÕES DE CONTAS E TÉCNICAS DE FORÇA BRUTA. A ANÁLISE DE TRÁFEGO DA REDE E O IDS/IPS DISTRIBUÍDO TRABALHAM JUNTOS PARA DETECTAR E RESPONDER A PROTOCOLOS ALTERNATIVOS UTILIZADOS PARA COMUNICAÇÃO E EXTRAÇÃO DE DADOS.

Em vez de apenas tentar parar o inevitável com appliances de hardware de perímetro físico, as equipes de segurança empresarial também devem concentrar os esforços no bloqueio da movimentação lateral assim que os malfeitores fizerem a violação inicial. Isso exige uma mudança fundamental em como a segurança é feita, com uma abordagem que requer a operacionalização da segurança leste-oeste em escala.

A oferta *NSX Advanced Threat Prevention* (ATP) da VMware para o *NSX Service-defined Firewall* oferece o mais amplo conjunto de recursos de detecção de ameaças que abrangem IDS/IPS de rede e análise de tráfego de rede com base em comportamento. Isso também inclui o VMware *NSX Advanced Threat Analyzer*™, uma oferta de sandbox que se baseia em uma tecnologia de emulação de sistema completo que tem visibilidade de cada ação de malware. O VMware NSX foi desenvolvido para proteger o tráfego do data center com as informações mais fiéis do setor sobre ameaças avançadas.

- A análise de tráfego de rede (NTA, pela sigla em inglês) aplica aprendizado de máquina (ML) não supervisionado ao tráfego de rede para detectar anomalias de tráfego e protocolo. A NTA também usa ML supervisionado para criar classificadores que reconhecem comportamentos de rede mal-intencionados e malwares anteriormente desconhecidos.
- O NSX aplica AI a comportamentos mal-intencionados e amostras de malware coletadas de sensores em toda a rede de inteligência de detecção de ameaças global NSX para criar e enviar automaticamente novas assinaturas IDS/IPS para todos os sensores NSX em escala de máquina.
- O NSX Advanced Threat Analyzer patenteado desconstrói todos os comportamentos projetados em um arquivo ou uma URL para determinar se são mal-intencionados. O NSX Advanced Threat Analyzer vê todas as instruções que um programa executa, bem como todo o conteúdo da memória e todas as atividades do sistema operacional.

Conclusão

É claro que os invasores estão fugindo do perímetro. A análise mostra que os invasores estão usando técnicas avançadas de evasão para contornar os controles de segurança e que, uma vez lá dentro, eles podem se espalhar sem serem detectados e intimidados até atingirem o objetivo, seja roubar informações ou causar interrupções. As equipes de segurança empresarial precisam de uma nova maneira de manter os usuários, aplicativos, dados e sistemas seguros, operacionalizando a segurança leste-oeste em escala.

As soluções de segurança do VMware NSX oferecem a visibilidade necessária para detectar ameaças dentro da rede, bem como os mecanismos para conter a propagação e limitar os danos. Como parte da arquitetura de segurança e confiança (Zero Trust) da VMware, o *NSX SDFW*, com recursos de *ATP*, combinado com a visibilidade no host e a detecção fornecida pelo *VMware Carbon Black EDR*, oferece uma oportunidade única de implantar uma solução de segurança abrangente que fornece a visibilidade e os controles de aplicação refinados para lidar com as ameaças que escapam do perímetro.

Análises de ameaças aprofundadas adicionais

A VMware Threat Analysis Unit (TAU) trabalhou em várias análises de ameaças aprofundadas. Os resultados da análise a seguir foram divulgados em postagens em blogs e apresentações em conferências.

Abordagem das vulnerabilidades da cadeia de fornecimento com uma arquitetura de segurança e confiança (Zero Trust)
Diante da violação da SolarWinds, esta análise ajuda os clientes que podem ter dúvidas sobre como uma arquitetura de segurança e confiança (Zero Trust) (ZTA, pela sigla em inglês) pode atuar como uma abordagem eficaz para limitar o impacto desses ataques.

Entender a violação da SolarWinds e as repercussões dela é um trabalho em andamento, e novos detalhes surgirão da análise de elementos e da telemetria.

Para mais informações, consulte: Reavaliação da sua postura de segurança após a violação da SolarWinds – *https://www.vmware.com/security/solarwinds-breach.html?src=WWW_US_HPHA_SolarWindsBreach_SiteLink*

A evolução da transformação da macro do Microsoft Excel 4.0 (XL4) em uma arma
A VMware TAU observou uma série de ondas de ataques que exploraram macros XL4 para comprometer os hosts. Essas macros estão se tornando cada vez mais populares entre os invasores, enquanto os fornecedores de segurança se esforçam para alcançá-las e detectá-las adequadamente.

Essa técnica abusa de um recurso legítimo do Microsoft Excel e não depende de nenhuma vulnerabilidade ou exploração. Para muitas organizações, bloquear esses arquivos não é uma solução viável, e todas as assinaturas para sinalizar essas amostras devem ser precisas o suficiente para não disparar em arquivos que aproveitam esse recurso de maneira legítima.

Como esse é um recurso que tem 30 anos e só foi descoberto e explorado em massa por invasores no ano passado, muitos fornecedores de segurança atualmente não têm mecanismos de detecção para disparar nessas amostras. Criar assinaturas confiáveis para esse tipo de ataque não é uma tarefa fácil. A análise mostra milhares de amostras se aproveitando dessa técnica, após monitorar e acompanhar a evolução delas por seis meses. A interceptação dessas amostras forneceu dados valiosos para criar estatísticas, identificar tendências, descobrir casos atípicos e acompanhar campanhas. Isso permite o agrupamento em clusters das amostras em ondas distintas, o que mostra claramente como essa técnica evoluiu ao longo do tempo para se tornar mais sofisticada e evasiva.

Como as macros XL4 representam um "território desconhecido", os autores de malwares estão introduzindo novos artifícios regularmente, ultrapassando os limites dessa técnica e identificando maneiras de evitar a detecção e ofuscar o código. As técnicas empregadas por esses invasores incluem maneiras de escapar da análise de sandbox automatizada e da detecção com base em assinatura, bem como da análise prática realizada por analistas de malwares e pelos responsáveis por fazer engenharia reversa. Como mencionado anteriormente, essas técnicas parecem surgir em ondas, com cada onda nova introduzindo novos artifícios que aproveitam o cluster ou a onda anterior. Uma série de postagens descreve cada onda e cluster em detalhes, mostrando cada técnica nova detectada e explicando por que cada uma é significativa.

Os resultados desta pesquisa foram apresentados na Virus Bulletin Conference (VB2020) em outubro de 2020.

A postagem original pode ser encontrada neste blog: *https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/*

Veja uma postagem de acompanhamento neste blog: *https://blogs.vmware.com/networkvirtualization/2020/10/evolution-of-excel-4-0-macro-weaponization-continued.html/*

Artifício de ameaça: o ransomware Ryuk mira no setor de saúde

Em outubro de 2020, a Cybersecurity & Infrastructure Security Agency (CISA) publicou um aviso sobre possíveis futuros ataques de ransomware direcionados ao setor de saúde. Esse relatório levantou preocupações relacionadas aos recursos escassos de hospitais e centros de atendimento devido à pandemia. Como consequência, um ataque de ransomware, além de paralisar a infraestrutura de um provedor de saúde, pode realmente colocar em risco a vida dos pacientes.

O aviso descreve em detalhes as táticas, as técnicas e os procedimentos (TTPs, pela sigla em inglês) seguidos pelos agentes mal-intencionados. O ataque usa vários componentes de malware, como TrickBot, BazarLoader, Ryuk e Cobalt Strike para comprometer redes, criar cabeças de ponte e se mover lateralmente para que, em algum momento, um ataque de ransomware possa ser executado de maneira bem-sucedida.

O ransomware Ryuk tem uma abordagem direcionada, seleciona as vítimas entre empresas, hospitais e instituições governamentais e exige um resgate muito alto para a recuperação dos dados. O Ryuk usa AES-256 como algoritmo de criptografia simétrico e RSA 4096 como algoritmo assimétrico. Na maioria dos casos, as etapas iniciais da investida são ataques de engenharia social que induzem os usuários a executar downloaders (TrickBot e BazarLoader) e executá-los, que, por sua vez, fazem download do ransomware (Ryuk).

Uma análise aprofundada dos vários componentes de malware envolvidos foi realizada, bem como das evidências de rede associadas a essas ações. Os resultados mostram uma cadeia de destruição que envolve downloaders que usam uma longa cadeia de execução abrangendo diversos elementos, como DLLs e scripts do PowerShell para entregar a carga útil do ransomware.

Mais detalhes sobre essa ameaça podem ser encontrados nesta postagem do blog: *https://blogs.vmware.com/networkvirtualization/2020/11/ryuk-ransomware-targets-health-care-industry.html/*

Atualizações de malwares e ameaças cibernéticas da COVID-19

A VMware TAU cobriu ataques que tinham o tema da COVID-19 em duas análises diferentes. Em ambos os casos, a análise mostra ataques de engenharia social que se aproveitaram da ansiedade em torno da pandemia.

As fontes de ameaças têm estado muito ativas durante a pandemia global atual. No entanto, a investigação inicial realizada em maio [5] mostrou que o método de operação delas não é novidade: os invasores usam anexos de e-mail como o método inicial de infecção para, posteriormente, inserir ladrões de informações ou spywares. Os agentes mal-intencionados dependem muito de arquivos compactados, pois eles fornecem uma camada fina de proteção contra soluções de segurança legadas ou neutralizadas que não conseguem extrair formatos de arquivo menos usados e processar corretamente o conteúdo deles.

A maioria dos ladrões de informações segue o modelo “malware como serviço” e é vendida por preços muito acessíveis em mercados clandestinos. Por isso, o principal diferenciador entre as diferentes campanhas acaba sendo a configuração do malware e não o código em si. Em vez disso, o que muda constantemente com o tempo é o empacotador encarregado de impedir que o malware seja detectado pelo maior tempo possível. As iterações mais recentes têm entregado cargas úteis baixadas de plataformas hospedadas publicamente (como os serviços de armazenamento on-line Google Drive™ ou Microsoft OneDrive), dificultando a identificação e o bloqueio do tráfego de rede resultante.

Em comparação com os ataques centrados em ladrões de informações relatados em maio [5], houve uma mudança para ameaças mais sofisticadas nos meses seguintes, como o NanoCore RAT modular e o infame Emotet [6]. Na campanha Emotet com o tema da COVID-19, o grupo Emotet abusou dos metadados de legenda em um objeto de formulário para ocultar uma string de script mal-intencionada do PowerShell. A cadeia de infecção geral é semelhante a outras campanhas Emotet relatadas [3], mas a análise também mostra alguns artifícios diferentes nessa variante, como abusar de um controle de quadro em vez de um objeto de várias páginas para armazenar a string de script do PowerShell e usar o cmdlet Invoke-Item para executar a carga útil do Emotet em vez de chamar o método de criação pela classe win32_process.

Conforme a pandemia continua, espere que as fontes de ameaças, incluindo o grupo Emotet, continuem aproveitando o tema da COVID-19 e desenvolvendo TTPs para lançar novos ataques.

Mais detalhes podem ser encontrados nesta postagem: *https://blogs.vmware.com/networkvirtualization/2020/11/covid-19-cyberthreat-and- malware-updates.html/*

Essa postagem é a continuação de uma análise anterior, descrita aqui: *https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/*

Derrote ataques Emotet com proteção contra malwares com base em comportamento

A comunidade de segurança desfrutou de alguns meses sem ouvir falar do Emotet, uma ameaça avançada e evasiva que começou em fevereiro de 2020. Mas esse silêncio foi quebrado em julho passado, quando a VMware TAU observou uma nova campanha importante do Emotet. O que chamou a atenção da VMware TAU foi que, como um todo, a comunidade de segurança ainda não tem capacidade para detectar e prevenir efetivamente o Emotet, embora ela tenha surgido inicialmente em 2014.

Nos ataques Emotet discutidos aqui, o grupo aproveitou várias técnicas para maximizar a taxa de infecção. Como visto em ataques típicos do Emotet, o processo de infecção começa com uma campanha de spam que utiliza e-mails de phishing com documentos de Word anexados como arma. As descobertas mostram que as técnicas de evasão usadas nos ataques (como macros VBA bastante ofuscadas e aproveitamento de controles de formulário, como legenda de várias páginas, para ocultar um script mal-intencionado do PowerShell) provaram ser muito eficazes para derrotar detecções com base em assinatura. Isso impõe grandes desafios aos controles de segurança tradicionais, que dependem muito de assinaturas para detectar ameaças. Por outro lado, as abordagens com base em comportamento, como a solução de sandbox de última geração orientada por AI da VMware, mostram grande eficácia em impedir ataques como os que aproveitam as técnicas discutidas acima.

Os detalhes dessa pesquisa podem ser encontrados aqui: *https://blogs.vmware.com/networkvirtualization/2020/11/defeat-emotet-attacks-with-behavior-based-malware-protection.html/*

VelvetSweatshop: as senhas padrão ainda podem fazer a diferença

Durante os meses de outubro e novembro de 2020, a VMware TAU observou um aumento na detecção de arquivos de Excel criptografados. Em geral, os documentos do Office podem ser protegidos por senha com o uso de um mecanismo de criptografia de chave simétrica que envolve uma senha que é a chave para criptografar e descriptografar o arquivo.

Os criadores de malwares usam essa chave como uma técnica de evasão adicional para ocultar o código mal-intencionado dos mecanismos de varredura antivírus. O problema é que criptografar um arquivo apresenta a desvantagem de exigir que a vítima em potencial insira uma senha (que normalmente está incluída no e-mail de phishing ou spam que contém o anexo criptografado). Isso deixa o e-mail e o anexo muito suspeitos, reduzindo bastante a chance de que a vítima abra o anexo mal-intencionado criptografado.

No entanto, os invasores estão usando um recurso obscuro do Excel que descriptografa automaticamente uma planilha criptografada sem pedir senha se a senha para criptografia for VelvetSweatshop. Essa é uma chave padrão armazenada no código do programa do Excel para descriptografia. É um artifício interessante que os invasores podem aproveitar para criptografar arquivos de Excel mal-intencionados a fim de evitar sistemas de detecção com base em análise estática, eliminando a necessidade de uma vítima em potencial inserir uma senha.

A chave de descriptografia incorporada no Excel não é um segredo. Ela é amplamente divulgada há muitos anos. No entanto, vê-la ainda ativa e extensivamente utilizada nos fez questionar a eficácia dos mecanismos modernos de varredura de antivírus para lidar com arquivos de Excel mal-intencionados criptografados.

Vários testes foram realizados para ver como a eficácia da detecção dos mecanismos de antivírus existentes muda quando os arquivos de Excel são criptografados, quando a criptografia é removida e quando um nível diferente de criptografia é usado. Os resultados foram um tanto surpreendentes. Mesmo que o uso da chave padrão seja uma técnica de evasão conhecida, ela ainda é muito eficaz, especialmente ao usar a criptografia AES-256.

Os detalhes da análise podem ser encontrados nesta postagem: *https://blogs.vmware.com/networkvirtualization/2020/11/velvetsweatshop-when-default-passwords-can-still-make-a-difference.html/*

O ransomware Snake
Durante o mês de junho de 2020, a VMware TAU descobriu um malware sofisticado e direcionado pertencente à família de ransomwares Snake. O malware é escrito na linguagem Go e é bastante ofuscado. As strings codificadas são criptografadas, o código-fonte é ofuscado e o ransomware tenta impedir o antivírus, as ferramentas de segurança de endpoints e os componentes de monitoramento e correlação.

O ransomware Snake é distribuído por meio de uma campanha focada e direcionada que se concentra exclusivamente em redes empresariais. A família de ransomwares tem laços com o Irã e é observada historicamente tendo como alvo infraestruturas críticas, como sistemas ICS e SCADA. Mais recentemente, o malware foi observado visando a organizações de saúde.

O ransomware nesta análise visou especificamente à rede empresarial de um fabricante de automóveis japonês. O ransomware parece ter como alvo principal os servidores, pois tem lógica para verificar o tipo de host que está infectando e tenta interromper muitos serviços e processos específicos de servidores.

Os detalhes da análise podem ser encontrados neste relatório: *https://blogs.vmware.com/networkvirtualization/files/2020/11/Targeted-Snake- Ransomware.pdf*

BitRansomware, que utiliza o Phorpiex, tem como alvo universidades da região APAC
O BitRansomware (também conhecido como DCryptSoft ou Readme) é, como o nome indica, um programa de ransomware que apareceu pela primeira vez em julho de 2020. Visando inicialmente a usuários que falam inglês, essa fonte de ameaças recentemente expandiu os ataques à região APAC, em particular com foco em universidades no Japão e em Hong Kong.

Como o ataque do ransomware Nemty informado no ano passado [7], o ataque do BitRansomware foi entregue com uma campanha de e-mail enorme realizada pelo botnet Phorpiex. A campanha de malspams distribuiu inúmeros arquivos ZIP que continham downloaders de ransomware em executáveismal-intencionados.

Como mostra a análise, a fonte de ameaças se aproveitou de várias técnicas para maximizar a taxa de infecção do ataque. O ataque começava com uma campanha de spam e, se o anexo era ativado, fazia download e exibia uma imagem na tela da vítima enquanto também fazia download da variante Phorpiex real de um dos hosts de comando e controle. Após a execução, a carga útil do Phorpiex descartava a cópia final do BitRansomware adquirida em um servidor C2.

Os detalhes da análise podem ser encontrados neste relatório: *https://blogs.vmware.com/networkvirtualization/threat-intelligence/*

Bibliografia

1. J. Zhang and S. Ortolani: “Phorpiex-Powered BitRansomware Targets APAC Universities”, VMware, 10/12/2020. [On-line]. Disponível em: https://blogs.vmware.com/ networkvirtualization/threat-intelligence/.
2. J. Zhang and S. Ortolani: “VelvetSweatshop: Default Passwords Can Still Make a Difference”, VMware, 19/11/2020. [On-line]. Disponível em: https://blogs.vmware.com/ networkvirtualization/2020/11/velvetsweatshop-when-default-passwords-can-still-make-a-difference.html/.
3. J. Zhang: “Defeat Emotet Attacks with Behavior-Based Malware Protection”, VMware, 5/11/2020. [On-line]. Disponível em: https://blogs.vmware.com/ networkvirtualization/2020/11/defeat-emotet-attacks-with-behavior-based-malware- protection.html/.
4. Symantec Security Response: “Living off the Land: Attackers Leverage Legitimate Tools for Malicious Ends”, Broadcom, 24/12/2019. [On-line]. Disponível em: https:// symantec-enterprise-blogs.security.com/blogs/threat-intelligence/living-land-legitimate-tools-malicious.
5. S. Sarkar, J. Zhang and S. Ortolani: “InfoStealers Weaponizing COVID-19”, Lastline (now part of VMware), 11/5/2020. [On-line]. Disponível em: https://www.lastline.com/ labsblog/infostealers-weaponizing-covid-19/.
6. J. Zhang, S. Sarkar and S. Ortolani: “COVID-19 Cyberthreats and Malware Updates”, VMware, 9/11/2020. [On-line]. Disponível em: https://blogs.vmware.com/ networkvirtualization/2020/11/covid-19-cyberthreat-and-malware-updates.html/.
7. J. Zhang and S. Ortolani: “Nemty Ransomware Scaling UP: APAC Mailboxes Swarmed by Dual Downloaders”, Lastline (agora parte da VMware), 18/2/2020. [On-line]. Disponível em: https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes- swarmed-dual-downloaders/.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Rua Surubim, 504 4º andar CEP 04571-050 Cidade Monções – São Paulo – SP Tel: (+55) 11 5509-7200 www.vmware.com/br

Item nº: VMware_Threat_Landscape_final_BR 6/21