BOLETIM DE SEGURANÇA

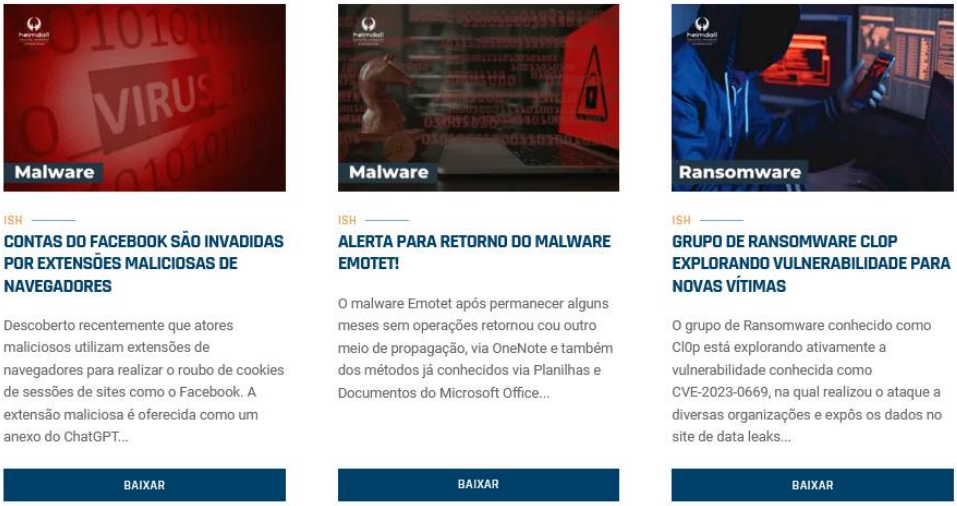
Novo trojan bancário Octo2 para Android avança em aquisição de dispositivos

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

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

Boletins de Segurança – Heimdall



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Pesquisadores de segurança cibernética identificaram uma nova versão do trojan bancário para Android, conhecido como Octo. Esta versão aprimorada, chamada Octo2, possui capacidades avançadas para aquisição de dispositivos (DTO) e execução de transações fraudulentas.

2 INFORMAÇÕES SOBRE A AMEAÇA

O Octo (ExobotCompact) é uma família de malware proeminente no atual cenário de ameaças móveis, liderando em número de amostras únicas observadas pelo ThreatFabric neste ano. A descoberta de uma nova versão, denominada “Octo2” por seu criador, pode alterar significativamente o panorama das ameaças e o modus operandi dos cibercriminosos. Este relatório detalha o estado atual da família de malware, destaca as atualizações e faz previsões para o futuro do Octo (ExobotCompact).

Principais Conclusões da Descoberta:

- Uma nova variante, chamada Octo2, da família de malware mais prevalente, foi lançada pelo agente de ameaça original.
- Desenvolvedores de malware aprimoraram a estabilidade dos recursos de ação remota necessários para ataques de aquisição de dispositivos.
- Novas campanhas Octo2 foram detectadas em países europeus.
- Octo2 utiliza técnicas avançadas de ofuscação para permanecer indetectável, incluindo a introdução do Algoritmo de Geração de Domínio

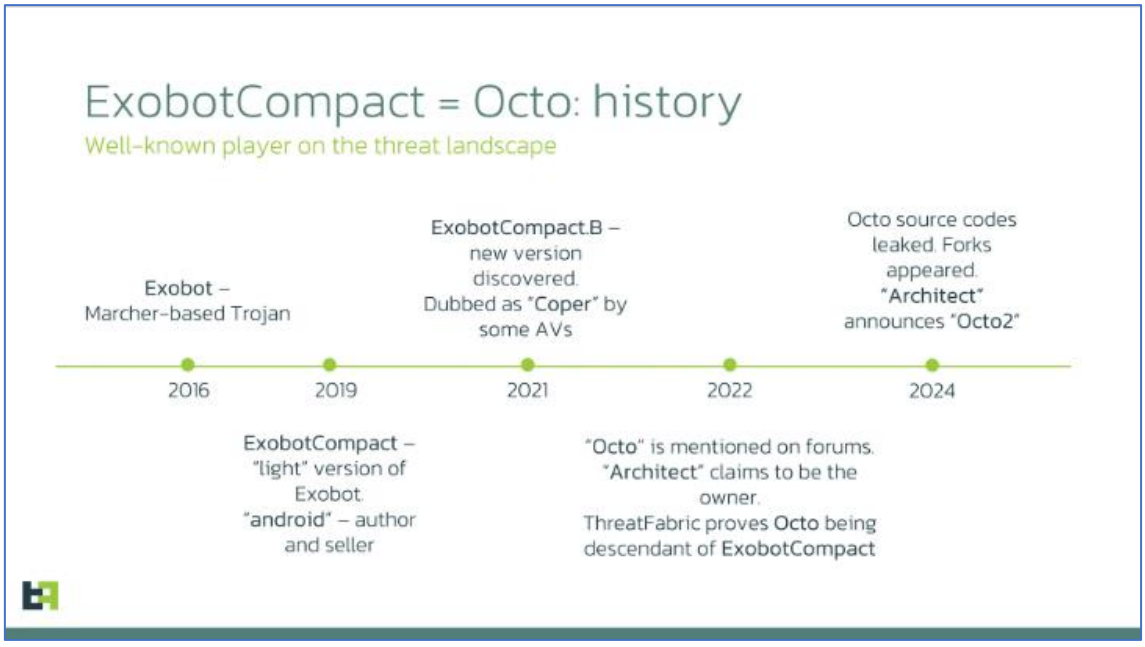


Figura 1 – Breve história do malware.

O malware Exobot surgiu pela primeira vez em 2016, sendo identificado como um trojan bancário. Nessa época, ele era capaz de realizar ataques de sobreposição e controlar chamadas, SMS e notificações push. Já em 2019, uma nova versão chamada "ExobotCompact" foi promovida em fóruns clandestinos, destacando-se por ser uma versão mais leve, mas ainda assim carregando a maioria das funcionalidades da versão original.

Após um período de inatividade, em 2021, uma nova variante do ExobotCompact foi descoberta. Alguns fornecedores de antivírus a denominaram "Coper", mas especialistas da ThreatFabric conseguiram rastrear a origem e confirmar a ligação com o ExobotCompact. Em 2022, começaram a surgir menções a uma nova família de malware, conhecida como "Octo", em fóruns underground. Um indivíduo sob o pseudônimo "Architect" afirmava ser o criador do Octo, mas forneceu poucos detalhes. Contudo, o ThreatFabric, ao analisar as informações limitadas disponíveis, estabeleceu que o Octo era apenas um novo nome para o ExobotCompact.

Desde então, a atividade envolvendo o Octo cresceu significativamente. Em 2022, mais campanhas relacionadas a ele foram detectadas, e novos criminosos cibernéticos começaram a utilizar essa ameaça, atraídos por suas capacidades, especialmente de acesso remoto, que eram constantemente atualizadas.

Em 2024, dois eventos importantes ocorreram no cenário das ameaças móveis envolvendo o Octo. Primeiro, o código-fonte do malware vazou, o que resultou na criação de várias versões derivadas. Esse vazamento também foi um dos motivos que levou ao segundo acontecimento marcante: o lançamento da nova versão do malware, conhecida como Octo2, feita pelo próprio criador original.

Nos últimos anos, o monitoramento da atividade do Octo revelou que variantes anteriores foram utilizadas em campanhas globais, atingindo diversas regiões, como Europa, Estados Unidos, Canadá, Oriente Médio, Cingapura e Austrália. A ThreatFabric acompanhou essas campanhas executadas pelos "clientes" do Octo Malware-as-a-Service. Com o anúncio da atualização para o Octo2, o proprietário do serviço informou que os usuários do Octo1 poderão migrar para a nova versão sem custos adicionais, com acesso antecipado. É esperado que os operadores do Octo1 façam essa transição, ampliando a presença do Octo2 no cenário de ameaças cibernéticas global.

A análise mostrou que as configurações do Octo2 incluem vestígios de vários aplicativos que estão no radar de interesse dos cibercriminosos. Isso foi identificado a partir da lista de nomes de pacotes recebidos do servidor de comando e controle (C2) como parte da configuração inicial, conhecida como "block_push_apps". Assim que o Octo2 detecta uma notificação push de algum aplicativo listado, ele a intercepta, impedindo que a vítima veja. A inclusão de um aplicativo nessa lista indica que ele já está sendo visado pelos cibercriminosos, provavelmente como parte de uma configuração padrão desenvolvida pelos criadores do malware.

Segundo nossa Inteligência de Ameaças, as primeiras amostras do Octo2 observadas em ambientes reais surgiram na Itália, Polônia, Moldávia e Hungria. Nessas campanhas iniciais, o malware se disfarçava como aplicativos legítimos, como Google Chrome, NordVPN e “Enterprise Europe Network”. No entanto, espera-se que os operadores por trás do Octo2 expandam suas operações, continuando a focar em usuários de serviços bancários móveis ao redor do mundo.

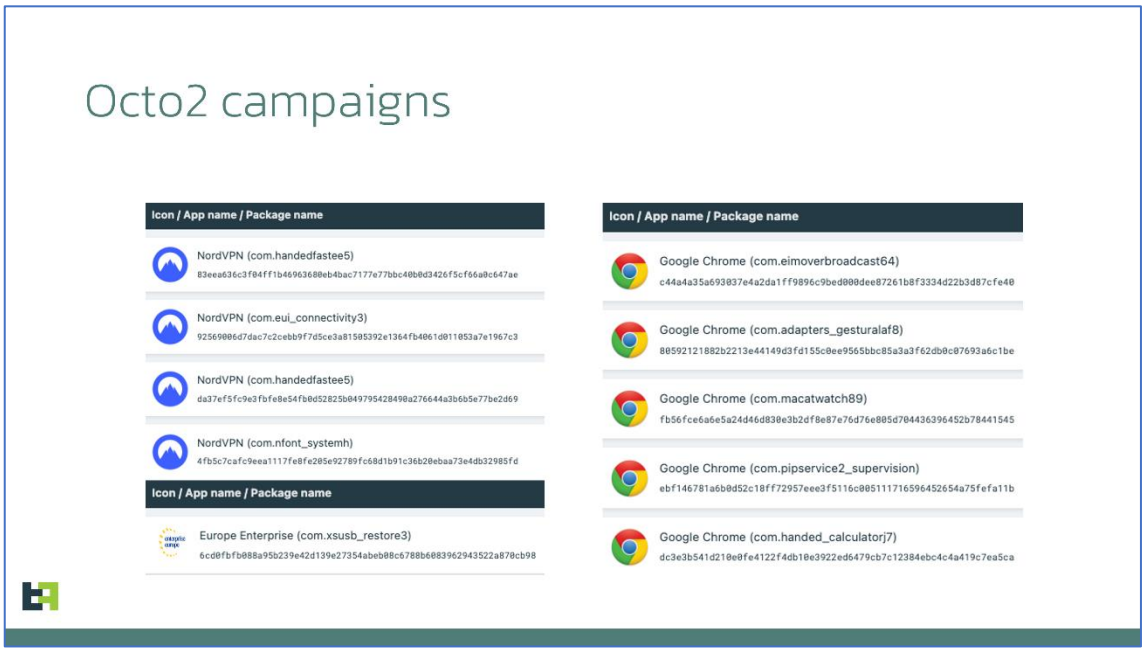


Figura 2 – Campanha do malware.

Nas campanhas identificadas pela ThreatFabric como Octo2, foi observado que o Zombinder desempenha o papel inicial no processo de infecção. Quando acionado, ele solicita que o usuário instale um "plugin" extra, que na realidade é o próprio malware Octo2. Esse mecanismo tem se mostrado eficaz em driblar as limitações impostas pelo Android 13 e versões superiores, permitindo que o malware se infiltre no dispositivo sem ser detectado. O Zombinder atua, portanto, como uma porta de entrada crucial, facilitando a instalação do Octo2 sob o disfarce de um componente aparentemente inofensivo, mas malicioso.

Desenvolvedores de malware e aqueles que oferecem malware como serviço enfrentam um desafio semelhante ao de empresas legítimas de software: como tornar seu "produto" mais atraente do que o dos concorrentes? Para o Octo, a competição é ainda mais intensa devido ao vazamento de seu código-fonte, o que significa que agora ele compete com sua própria versão gratuita no mercado ilícito. Isso levou os criadores do Octo2 a aprimorarem significativamente o "produto" para garantir sua relevância e popularidade.

Não surpreende, portanto, que o Octo2 tenha recebido atualizações importantes em comparação com suas versões anteriores. As mudanças focaram principalmente em aprimorar a estabilidade durante ataques de Controle Remoto do Dispositivo (Device Takeover) e em melhorar as técnicas antidetecção e antianálise. Entre as melhorias, destaca-se a maior estabilidade do RAT (Remote Access Trojan). Os desenvolvedores implementaram ajustes para reduzir a latência em sessões remotas, permitindo que os operadores definam uma configuração de "qualidade baixa" para limitar a quantidade de dados transmitidos ao servidor de comando e controle (C2). Isso melhora o desempenho em redes instáveis, reduzindo a qualidade das capturas de tela enviadas, o que ajuda a manter a conexão estável.

O Octo2 também apresentou avanços em suas técnicas anti-análise e anti-detecção. Enquanto o Octo original já era conhecido por sua ofuscação avançada de código, o Octo2 introduz um processo ainda mais sofisticado, com várias camadas de descriptografia e carregamento dinâmico de bibliotecas nativas. Esse processo dificulta o trabalho de analistas e sistemas de segurança ao tentarem identificar e neutralizar o malware.

Outra inovação do Octo2 é o uso de um Algoritmo de Geração de Domínio (DGA), que gera dinamicamente os domínios do servidor C2, facilitando a atualização e substituição de domínios quando necessário. Embora essa abordagem tenha limitações conhecidas, como a possibilidade de pesquisadores preverem domínios futuros, o Octo2 implementa um algoritmo proprietário baseado em data, dificultando a previsão.

Por fim, a comunicação com o C2 também foi aprimorada. O Octo2 agora gera uma nova chave de criptografia para cada solicitação enviada ao servidor, tornando mais difícil a interceptação e descriptografia dos dados por sistemas de defesa. Com esses avanços, o Octo2 representa um desafio crescente para a segurança de mobile banking, pois suas capacidades aumentadas e ofuscação complexa tornam o malware mais resiliente, prolongando seu impacto e dificultando sua detecção e remoção pelos sistemas de segurança.

3 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Mantenha o sistema Android atualizado

- Certifique-se de que o sistema operacional e os aplicativos instalados estejam sempre atualizados para corrigir vulnerabilidades exploradas por trojans como o Octo2.

Use autenticação de dois fatores (2FA)

- Habilite a autenticação multifator em suas contas bancárias e outros serviços sensíveis para adicionar uma camada extra de proteção, dificultando o acesso de cibercriminosos.

Baixe aplicativos apenas de fontes confiáveis

- Evite instalar aplicativos de terceiros ou de lojas de aplicativos não oficiais. Baixe apenas da Google Play Store ou de fontes verificadas para reduzir o risco de instalar aplicativos maliciosos.

Monitore permissões de aplicativos

- Verifique regularmente as permissões concedidas aos aplicativos instalados e evite dar permissões excessivas, como acesso a SMS, contatos e histórico de chamadas, que podem ser usados por trojans bancários para roubar informações.

Utilize soluções de segurança confiáveis

- Instale e mantenha um software de segurança móvel atualizado em seu dispositivo para detectar e bloquear ameaças como o Octo2 antes que possam causar danos.

Phishing e golpes por SMS

- Evite clicar em links suspeitos recebidos via SMS, e-mails ou mensagens instantâneas, que podem redirecionar para o download de malware disfarçado de aplicativos bancários.

Evite usar redes Wi-Fi públicas

- Redes abertas e não seguras podem ser usadas para interceptar dados transmitidos. Sempre use uma conexão VPN quando precisar acessar informações confidenciais em redes públicas.

4 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	e32eeea3676874431571f976d044a816
sha1:	d40169c63e74d86cc0d02c638401bcd9ccdb621b
sha256:	83eea636c3f04ff1b46963680eb4bac7177e77bbc40b0d3426f5cf66a0c647ae
File name:	NordVPN_2.66.apk

Indicadores de compromisso do artefato	
md5:	c508d432e3d521acaa6215934f609b2a
sha1:	5e44ba99e81c6673b000519755e041c2d4082ae8
sha256:	6cd0fbfb088a95b239e42d139e27354abeb08c6788b6083962943522a870cb98
File name:	Europe Enterprise.apk

Indicadores de compromisso do artefato	
md5:	11cb1b221952268fcd6000e563752d79
sha1:	d4a85997999a975848b60fd52597538baf652daf
sha256:	117aa133d19ea84a4de87128f16384ae0477f3ee9dd3e43037e102d7039c79d9
File name:	11cb1b221952268fcd6000e563752d79.virus

Tabela 1 – Indicadores de Compromissos de artefatos

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Threatfabric**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH