heimdall

security research

A DIVISION OF ISH

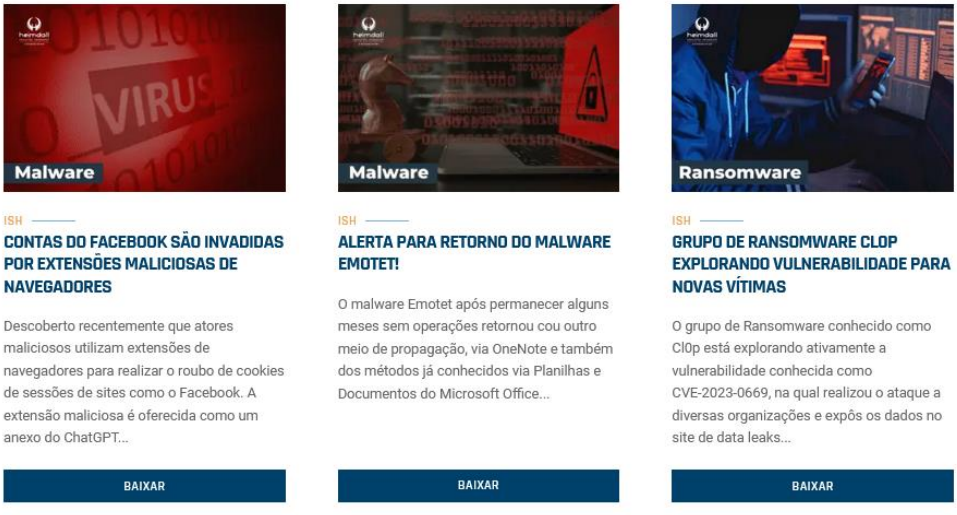
Campanha maliciosa contra Iphones na Rússia

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

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 NOVO SPYWARE?

Na data de primeiro de junho, o CEO da Kaspersky realizou a publicação no blog da empresa afirmando que os especialistas identificaram um ataque cibernético extremamente complexo e direcionado a profissionais que utilizam os dispositivos móveis da Apple.

Segundo Eugene, o objetivo do ataque é a introdução discreta de spyware nos iPhones dos funcionários da empresa.

O ataque se iniciava com uma mensagem por meio do iMessage invisível com um anexo malicioso, que utilizando várias vulnerabilidades no sistema operacional iOS, é executado no dispositivo e instala o spyware. A implantação do spyware é totalmente oculta e não requer nenhum tipo de ação do usuário. Além disso, o spyware também realiza a transmissão silenciosamente de informações privadas para servidores remotos: gravações de microfone, fotos de mensagens instantâneas, geolocalização e dados sobre várias outras atividades do proprietário do dispositivo infectado.

O ataque foi detectado pela plataforma da Kaspersky (PUMA), identificado a atuação do ataque de forma discreta, onde o sistema detectou uma anomalia na rede de dispositivos Apple e uma investigação mais aprofundada da equipe identificou que várias dezenas de iPhones dos colaboradores foram infectados com o novo spyware, o qual foi apelidado como “Triangulation”.

Devido a natura do iOS, não há (e não poderá haver) nenhuma ferramenta padrão do sistema operacional para detectar e remover o spyware em smartphones infectados.

Uma indicação da presenta do malware é a desativação da capacidade de atualizar o iOS.

A Kaspersky forneceu um relatório sobre a operação com os dados capturados sobre a campanha maliciosa até o momento.

2 SOBRE O ATAQUE

Os backups de dispositivo móveis contêm uma cópia parcial do sistema de arquivos, incluindo alguns dados de usuários e banco de dados de serviço. Os registros de data e hora dos arquivos, pastas e registros do bancod e dados permitem reconstruir aproximamdanente os eventos que acontecem no dispositivo. O utilitário de linha de comando “mvt-ios” produz uma linha do tempo classificada de eventos em um arquivo chamado “timeline.csv”, semelhante a uma super linha de tempo usada.

Utilizando essa linha do tempo, os analistas da Kaspersky conseguiram identificar artefatos específicos que indicam o comprometimento. Isso permitiu avançar a pesquisa e reconstruir a sequência geral da infecção:

- O dispositivo iOS de destino recebe uma mensagem por meio do serviço iMessage, com um anexo contendo um exploit;
- Sem nenhuma interação do usuário, a mensagem aciona uma vulnerabilidade que leva à execução do código;
- O código dentro do exploit baixa vários estágios subsequentes do servidor C2, que incluem exploits adicionais para escalonamento de privilégios;
- Após a exploração bem-sucedida, um payload final é baixado do servidor C2, a qual é uma plataforma APT com todos os recursos.
- A mensagem inicial e a exploração no anexo são excluídas.

O conjunto de ferramentas maliciosas não oferece suporte à persistência, provavelmente segundo os analistas devido ao Sistema Operacional. De acordo com a cronologia, foi verificar que os dispositivos podem ser infectados novamente após a reinicialização. Os vestígios mais antigos de infecção que foi descoberto aconteceu em 2019. Até o momento da análise o ataque ainda está em operação, sendo que a versão mais recente dos dispositivos visados com sucesso é o iOS 15.7.

3 ATIVIDADES DE REDE DESCOBERTAS

Quanto a evidências de rede, foi possível realizar a captura de tráfego de rede indicando uma sequência de vários eventos de conexão HTTPS.

- Interação de rede legítima com o serviço iMessage, geralmente usando os nomes de domínios ***.ess.apple.com**.
- Download do anexo do iMessage, usando os nomes de domínios **“.icloud-content.com e content.icloud.com”**.
- Múltiplas conexões aos domínios C2, geralmente com 2 domínios diferentes.

Time	Server Name	Destination	Destination Port	Protocol
222.577175	init.ess.apple.com	62.115.253.208	443	TLSv1.3
223.248546	kt-prod.ess.apple.com	17.145.0.2	443	TLSv1.3
250.471089	p113-caldav.icloud.com	17.250.84.36	443	TLSv1.2
301.339923	edge-102.sesto4.icloud-content.com	17.250.84.37	443	TLSv1.3
302.194211	p31-content.icloud.com	17.250.84.22	443	TLSv1.2
314.766744	setup.icloud.com	17.250.84.19	443	TLSv1.2
339.869951	backuprabbit.com	104.21.21.154	443	TLSv1.3
359.630968	gsa.apple.com	17.32.194.2	443	TLSv1.2
360.605764	backuprabbit.com	104.21.21.154	443	TLSv1.3
361.092903	pds-init.ess.apple.com	62.115.253.218	443	TLSv1.3
368.065719	cloudsponcer.com	104.21.79.172	443	TLSv1.3
377.414078	backuprabbit.com	104.21.21.154	443	TLSv1.3
423.442812	gateway.icloud.com	17.250.84.4	443	TLSv1.3
426.333906	identity.ess.apple.com	17.138.176.4	443	TLSv1.3
427.062256	identity.ess.apple.com	17.138.176.4	443	TLSv1.3
428.386581	identity.ess.apple.com	17.138.176.4	443	TLSv1.3
429.057571	identity.ess.apple.com	17.138.176.4	443	TLSv1.2
437.411511	iphone-ld.apple.com	62.115.253.233	443	TLSv1.3
500.156738	init.itunes.apple.com	184.51.132.49	443	TLSv1.3
760.068442	courier.push.apple.com	17.57.146.133	5223	TLSv1.3
761.825773	iphone-ld.apple.com	62.115.253.219	443	TLSv1.3
762.498958	cloudsponcer.com	104.21.79.172	443	TLSv1.3
765.125499	gs-loc.apple.com	17.36.206.4	443	TLSv1.3

Figura 1 – Tráfego de rede capturado.

O anexo do iMessage é criptografado e baixado por HTTPS, havendo a indicação apenas que a quantidade de dados baixados é cerca de **242KB.**

Figura 2 – Anexo criptografado do Exploit.

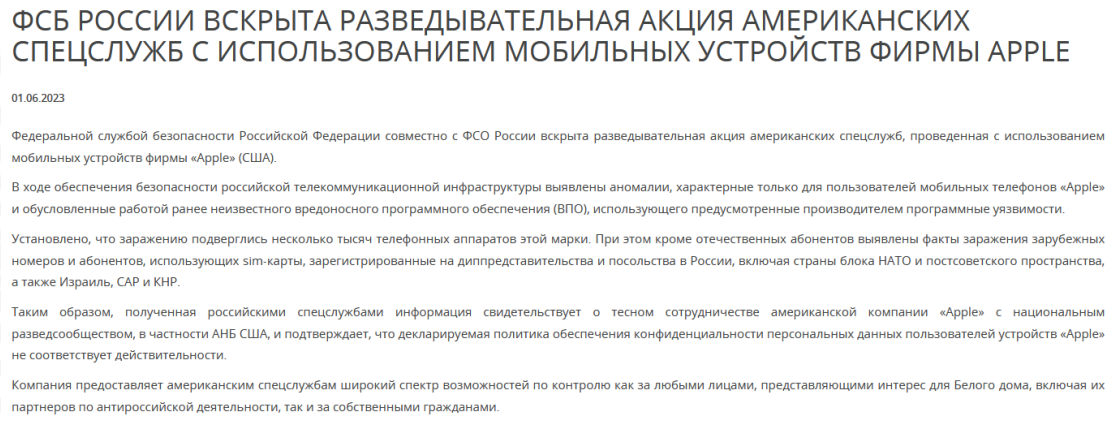
4 MANIFESTAÇÃO DO FSB

O Serviço Federal de Segurança da Rússia, publicou um alerta na qual mencionou a ação de reconhecimento de serviços de inteligência em dispositivos móveis da Apple.

Segundo o comunicado, o FSB afirmou que identificaram anomalias específicas para usuários de telefones celulares da Apple e causadas pela operação de software malicioso desconhecido que utiliza vulnerabilidades de softwares "fornecidas pelo fabricante".

Foi verificado que vários milhares de aparelhos telefônicos da marca estavam infectados e, ao mesmo tempo além de assinantes domésticos, foi identificado a infecção de números de estrangeiros assinantes com cartões SIM registrados na Rússia, incluindo os países do bloco da OTAN e o espaço pós-soviético, Isarel, SAR e China.

O FSB afirma que a Apple realizou a cooperação com as operações da NSA dos Estados Unidos.



ФСБ РОССИИ ВСКРЫТА РАЗВЕДЫВАТЕЛЬНАЯ АКЦИЯ АМЕРИКАНСКИХ СПЕЦСЛУЖБ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ ФИРМЫ APPLE

01.06.2023

Федеральной службой безопасности Российской Федерации совместно с ФСО России вскрыта разведывательная акция американских спецслужб, проведенная с использованием мобильных устройств фирмы «Apple» (США).

В ходе обеспечения безопасности российской телекоммуникационной инфраструктуры выявлены аномалии, характерные только для пользователей мобильных телефонов «Apple» и обусловленные работой ранее неизвестного вредоносного программного обеспечения (ВПО), использующего предусмотренные производителем программные уязвимости.

Установлено, что заражению подверглись несколько тысяч телефонных аппаратов этой марки. При этом кроме отечественных абонентов выявлены факты заражения зарубежных номеров и абонентов, использующих sim-карты, зарегистрированные на диппредставительства и посольства в России, включая страны блока НАТО и постсоветского пространства, а также Израиль, САР и КНР.

Таким образом, полученная российскими спецслужбами информация свидетельствует о тесном сотрудничестве американской компании «Apple» с национальным разведсообществом, в частности АНБ США, и подтверждает, что декларируемая политика обеспечения конфиденциальности персональных данных пользователей устройств «Apple» не соответствует действительности.

Компания предоставляет американским спецслужбам широкий спектр возможностей по контролю как за любыми лицами, представляющими интерес для Белого дома, включая их партнеров по антироссийской деятельности, так и за собственными гражданами.

Figura 3 – Manifestação do FSB Russo.

5 IoCs

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.

URLs de distribuição e endereços IP C2:

addatamarket[.]net
backuprabbit[.]com
businessvideonews[.]com
cloudsponcer[.]com
datamarketplace[.]net
mobilegamerstats[.]com
snoweeanalytics[.]com
tagclick-cdn[.]com
topographyupdates[.]com
unlimitedteacup[.]com
virtuallaughing[.]com
web-trackers[.]com
growthtransport[.]com
anstv[.]net
ans7tv[.]net

Tabela 1 – Indicadores de Rede C2 e download de artefatos

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Publicação Kaspersky sobre a Traingulação;**
- **Manifestação do FSB Russo.**

heimdall
security research

A DIVISION OF ISH