Отчет о тенденциях в области вредоносных программ, октябрь 2020 года

Этот отчет является ежемесячной сводкой группы сетевой криминалистики Varonis. В нем перечислена активность, наблюдаемая при реагировании на инциденты, проведении расследований сетевой криминалистики и обратной разработке образцов вредоносных программ. Данный отчет призван помочь лучше понять меняющийся ландшафт угроз и соответствующим образом адаптировать защиту.

Обзор вредоносных программ — Ryuk

[1] Ryuk — это разновидность программы-вымогателя, обнаруженная в августе 2018 года. Она отличается от других известных программ-вымогателей (например, WannaCry) тем, что используется в основном для целевых атак. Специфика Ryuk заключается в том, что злоумышленник уделяет каждой жертве индивидуальное внимание.

У хорошо известных модификаций Ryuk есть 2 основных способа заражения: использование специально созданных писем адресного фишинга, обычно нацеленных на определенный персонал внутри организации, а также использование заранее полученных учетных данных для доступа к устройствам внутри компании-жертвы через удаленный рабочий стол.

[2] Недавно было замечено, что Ryuk использует эксплойт Zerologon (CVE-2020-1472), который позволяет киберпреступникам повышать свои права намного быстрее, чем с помощью других способов. В результате нередко возникает ситуация, когда злоумышленник использует пароль первичного контроллера домена для бокового перемещения к остальным контроллерам домена и их дальнейшего использования для распространения программы-вымогателя по сети.

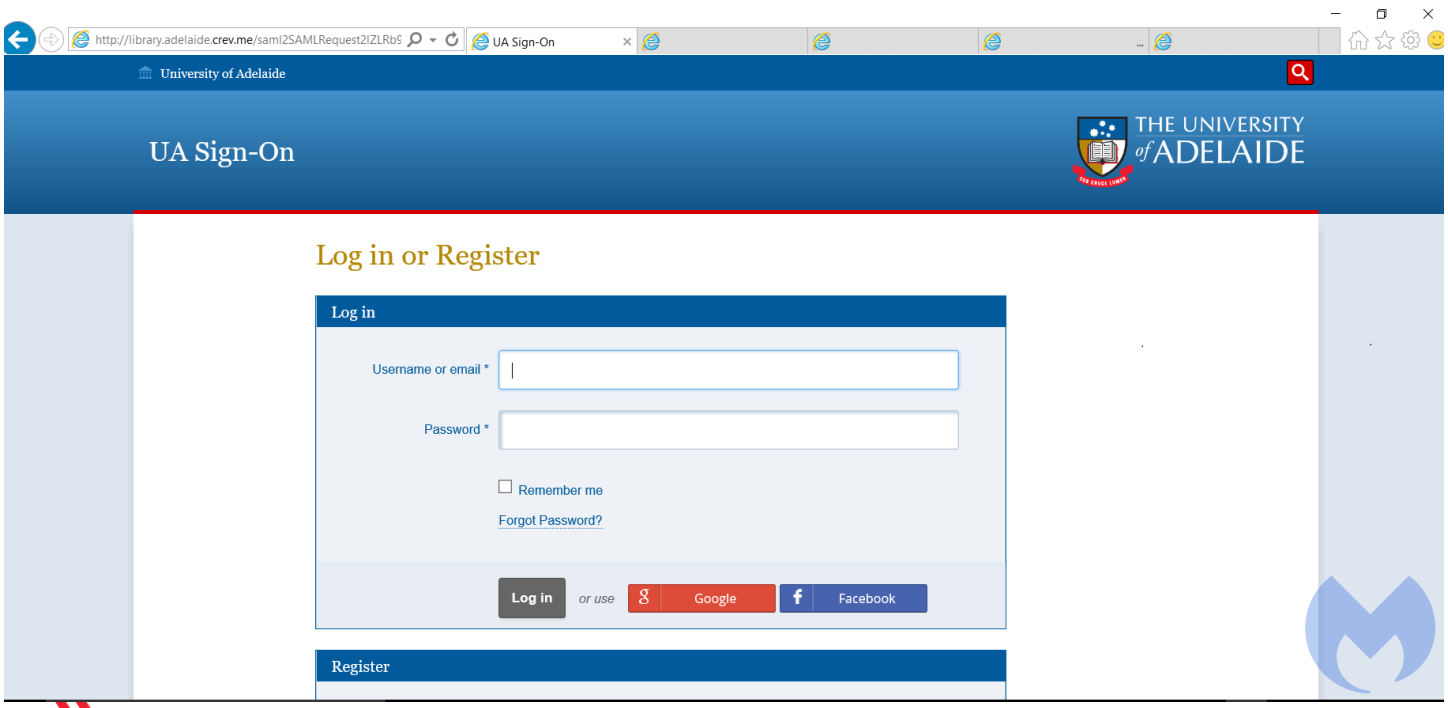
Обзор вредоносных программ — таргетированная атака Silent Librarian

[3] Злоумышленник Silent Librarian, также известный как COBALT DICKENS или TA407, использует методы адресного фишинга для атак на университеты (в основном в США, но также и в других частях мира). Его жертвами являются сотрудники и учащиеся университетов, а цель заключается в краже научно-исследовательских данных.

Silent Librarian базируется в Иране и, скорее всего, финансируется иранским правительством. Этот злоумышленник свидетельствует о намерениях Ирана идти в ногу с мировым научным прогрессом, даже несмотря на жесткие санкционные ограничения, с которыми столкнулась страна.

Чтобы заманить жертв в ловушку, Silent Librarian использует доменные имена, очень похожие на настоящее доменное имя университета, но при этом меняет доменное имя верхнего уровня на другое.

Например, домен Западного университета Канады (Western University Canada) — login.proxy1.lib.uwo.ca, а злоумышленники используют домен login.proxy1.lib.uwo.ca.sftt.cf. Для Библиотеки университета Аделаиды (University of Adelaide Library) настоящее доменное имя — library.adelaide.edu.au, а злоумышленник использует домен library.adelaide.crev.me. Вот как выглядит фишинговый сайт:



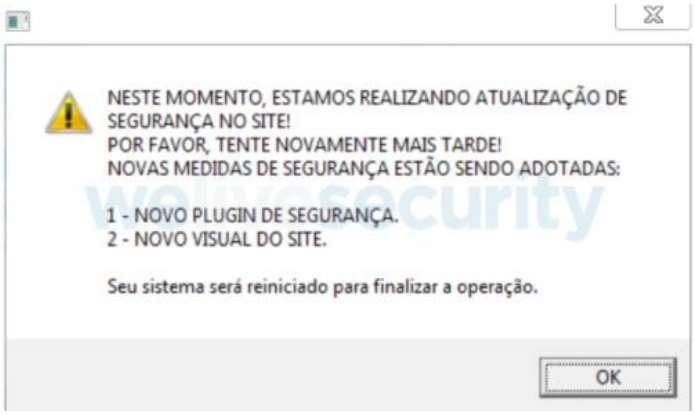
Silent Librarian использует сервис Cloudflare, чтобы скрыть информацию об источнике хостинга. Это связано с тем, что злоумышленники, как правило, используют инфраструктуру в собственной стране, скорее всего из-за недоступности инфраструктуры в других странах.

Обзор вредоносных программ — Mekotio

Mekotio — банковский троян, который впервые был обнаружен в 2015 году. В последние годы банковские трояны становятся все более распространенными благодаря внушительной полезной нагрузке при успешной реализации атаки.

[4] Чтобы оставаться незамеченными антивирусными программами и системами обнаружения угроз и реагирования на них, банковские трояны должны постоянно изменяться и развиваться. Латиноамериканский троян Mekotio является отличным примером этого правила: его набор функций часто меняется, и, более того, одновременно разрабатывается несколько разновидностей Mekotio. В основном троян Mekotio распространяется посредством спам-рассылок и использует несколько этапов загрузки.

В своих атаках для сбора конфиденциальной информации Mekotio использует специально созданные всплывающие окна, нацеленные на латиноамериканские банки. Mekotio обладает расширенными возможностями разведки для определения конфигурации брандмауэра, версии Windows, установленных решений безопасности и наличия у текущего пользователя административных прав. Он также использует стандартные методы для закрепления в системе с помощью ключей реестра или папки автозагрузки Windows.



Кроме того, в дополнение к обычным функциям, таким как запись нажатий кнопок и создание снимков экрана, он содержит несколько интересных возможностей: извлечение учетных данных, хранящихся в браузере Google Chrome, кража криптовалюты путем замены строк в буфере обмена и частичное уничтожение данных путем удаления файлов и папок в системных каталогах.

Из-за разницы в банковских системах в разных странах варианты банковских троянов, как правило, зависят от местоположения. Это относится и к Mekotio. Хотя его основными целями являются банки в Латинской Америке, известны десятки случаев, когда его жертвами становились и другие банки, в основном в Бразилии, Чили, Мексике и Перу.

Обнаружения Varonis

Varonis DatAlert имеет несколько моделей угроз, которые могут идентифицировать перечисленные выше виды вредоносных программ на разных этапах их деятельности:

- «**Обнаружена криптографическая деятельность**»: обнаруживает создание сообщений о выкупе на файловом сервере или в облачном хранилище данных.
- «**Обнаружена модель поведения, требующая срочного реагирования: действия пользователя напоминают действия программы-вымогателя**»: обнаруживает процесс шифрования файлов на файловом сервере, не полагаясь на известные имена или расширения файлов программы-вымогателя. Это позволяет обнаруживать новые разновидности программ-вымогателей и уничтожителей данных.
- «**Нестандартное поведение: на внешние сайты загружен необычный объем данных**»: проверяет объем отправляемой информации и обнаруживает загрузку собранных данных на веб-сайт за пределами домена организации.

- «**Возможная фишинговая атака: доступ к опасному сайту, доменное имя которого содержит необычные символы**»: обнаруживает, когда пользователь обращается к веб-сайту, который может содержать вредоносные программы, на основе необычных символов в URL-адресе сайта.
- «**Подозрительное электронное письмо: получено электронное письмо с предположительно вредоносным вложением**»: обнаруживает, когда вложение электронной почты может содержать вредоносный код или ссылку на вредоносный сайт.

История успеха

У одного из клиентов Varonis — химической компании с тысячами сотрудников — произошел инцидент, связанный с программой-вымогателем NetWalker.

В конце сентября группа сетевой криминалистики Varonis связалась с клиентом после того, как наши системы отслеживания угроз указали о потенциальной угрозе скрытой атаки с помощью программы-вымогателя.

В ходе расследования выяснилось, что у клиента был взломанный пользователь Office 365, которого злоумышленник использовал для получения доступа к локальной сети.

Попав в сеть, злоумышленник смог взломать учетную запись службы и использовать ее для запуска программ-вымогателей Cobalt Strike и NetWalker.

Вот как наша команда помогла клиенту:

- Вместе с заказчиком мы использовали возможности Varonis для анализа оповещений, чтобы убедиться, что все хранилища данных под контролем.
- Мы соотнесли известные фазы атаки с разрозненными событиями.
- Мы предоставили индикаторы компрометации (IOC) программы-вымогателя NetWalker, чтобы клиент смог провести расследование и в других системах кибербезопасности.
- Мы предоставили полный и исчерпывающий отчет о вредоносной программе, включая описание возможностей различных модификаций NetWalker. Эти данные мы получили путем обратной разработки образца, обнаруженного в рабочей среде клиента.

Новые разновидности программ-вымогателей, проанализированные в октябре

Название разновидности	Количество	Ориентированные на данные индикаторы компрометации
mechu ransomware	1	Расширение: .mechu4Po
Babaxed Ransomware	2	Расширение: .babaxed
Dharma ransomware	3	Расширение: .WSHLP
EasyRansom ransomware	1	Сообщение о выкупе: easyransom_readme.txt Расширение: .easyransom
STOP ransomware	3	Расширение: .lyli
Dharma ransomware	3	Расширение: .fresh
Mame VSE Ransomware	1	Расширение: .mame vse
Dharma ransomware	3	Расширение: .homer
Dharma ransomware	3	Расширение: .flyu
Babaxed Ransomware	2	Расширение: .osnoed
STOP Djvu ransomware	3	Расширение: .moss
SantaCrypt Ransomware	2	Сообщение о выкупе: HOW_TO_RECOVER_MY_FILES.TXT Расширение: .$anta
Curator ransomware	1	Расширение: .CURATOR
WoodRat ransomware	1	Расширение: .woodrat
Cyber_Splitter	1	Расширение: .Dcry
Dharma ransomware	3	Расширение: .gtsc
Snatch Ransomware	1	Extension: .clhmotjdxp
Nibiru Ransomware	1	Расширение: .Nibiru
Geneve Ransomware	1	Расширение: .fezmm
Ranzy Locker Ransomware	1	Расширение: .RNZ
Matrix Ransomware	3	Сообщение о выкупе: J91D_README.rtf Расширение: .J91D
Matrix Ransomware	3	Сообщение о выкупе: S996_INFO.rtf Расширение: .S996
Matrix Ransomware	3	Сообщение о выкупе: FDFK22_INFO.rtf Расширение: .FDFK22
Consciousness Ransomware	1	Сообщение о выкупе: Consciousness Ransomware Text
AIDS_NT Ransomware	1	Сообщение о выкупе: AIDS_NT_Instructions.txt
Xorist ransomware	2	Расширение: .emilisub
ThunderX	1	Расширение: .tx_locked
Xorist ransomware	2	Расширение: .hnx911
MedusaLocker	2	Расширение: .networkmaze
OGDO STOP	1	Расширение: .ogdo
Flamingo Ransomware	1	Расширение: .FLAMINGO
Dharma Ransomware	3	Расширение: .eur
Dharma Ransomware	3	Расширение: .blm
XMRLocker	1	Расширение:. [XMRLocker]

Основные векторы атак в октябре

Библиография

[1] - https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ryuk-ransomware/

[2] - https://threatpost.com/ryuk-ransomware-gang-zerologon-lightning-attack/160286/

[3] - https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/

[4] - https://www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/

Команда сетевой криминалистики Varonis

Дата составления отчета: октября 2020 г.

По любым вопросам и за дополнительной информацией обращайтесь к нам по адресу:

dl-eng-forensics@varonis.com