Атаки, использующие доверенную корпоративную инфраструктуру для кражи учетных данных в сетях АСУ

Кирилл Круглов

19.01.2022 Version 1.1

«Аномальные» атаки с использованием шпионских программ 2
Анализ шпионских программ 4
Инфраструктура сбора данных 4
Тактика, методы и процедуры 6
Организаторы атак 10
Разработчики вредоносного ПО и поставщики услуг по схеме «Шпионское ПО как сервис» 13
Торговые площадки 16
Заключение 19
Рекомендации 20
Приложение I — Индикаторы компрометации 21

В 2021 году специалисты ICS CERT обратили внимание на растущее множество аномальных атак с применением шпионского ПО, которым заражаются компьютеры АСУ по всему миру.

Несмотря на то, что вредоносные программы, применяемые в этих атаках, являются широко распространенным шпионским ПО, сами атаки выделяются из общей массы очень ограниченным числом целей у каждой атаки и очень коротким временем жизни каждого вредоносного образца, что и составило суть обнаруженной аномалии.

К моменту обнаружения аномалию уже можно было считать тенденцией: около 21,2% всех образцов шпионского ПО, заблокированных в первой половине 2021 года на компьютерах АСУ по всему миру, относились к новой серии атак с ограниченным охватом и коротким временем жизни. В то же время, в зависимости от региона, одновременно до одной шестой части всех компьютеров, подвергавшихся атакам шпионского ПО, было атаковано именно с применением этой тактики.

В ходе исследования аномалии мы обнаружили большое число кампаний, в которых вредоносное ПО распространяется от одного промышленного предприятия к другому через фишинговые письма, замаскированные под корреспонденцию организаций-жертв. При этом злоумышленники использовали корпоративные почтовые системы этих организаций для осуществления атак по спискам контактов, украденным из взломанных почтовых ящиков.

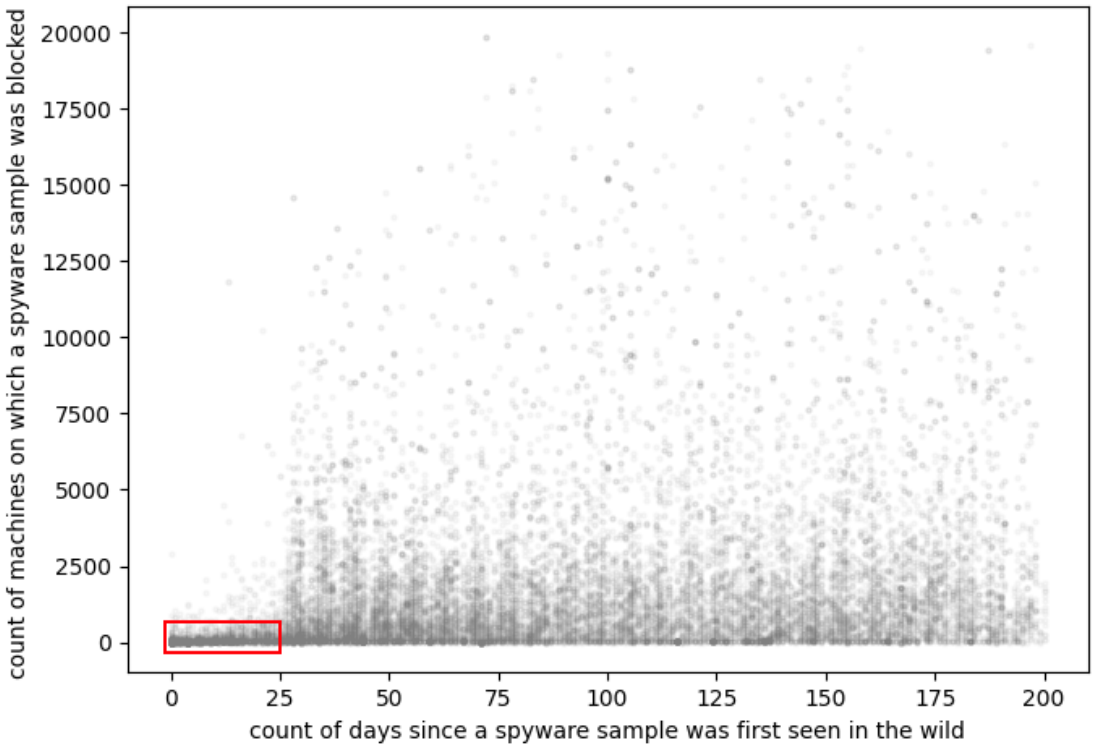
В общей сложности мы обнаружили более 2 000 корпоративных почтовых аккаунтов, принадлежащих промышленным компаниям и задействованных в результате подобной вредоносной активности в качестве серверов для проведения последующих атак. В то же время, по нашей оценке, количество украденных аккаунтов гораздо больше (порядка 7 000).

Полный текст отчёта опубликован на портале Kaspersky Threat Intelligence.
Если вам нужно больше информации, напишите нам: ics-cert@kaspersky.com.

«Аномальные» атаки с использованием шпионских программ

Расскажем подробнее об аномалии. Анализ 58 586 образцов программ-шпионов, заблокированных в первом полугодии 2021 года, показал, что 12 420 (21,2%) из них были значительно меньше распространены (по общему количеству компьютеров, на которых был заблокирован образец вредоносного ПО, включая компьютеры, не связанные с АСУ), а промежуток времени (в днях) между первой и последней датой обнаружения вредоносного ПО — значительно короче, чем в обычных атаках шпионского ПО. Показатели таких «аномальных» шпионских программ отмечены красным прямоугольником на графике ниже. Видно, что продолжительность атак невелика и, как правило, не превышает 25 дней. При этом количество атакованных компьютеров составляет менее 100, из которых 40-45% — это машины АСУ, а остальные чаще всего являются частью ИТ-инфраструктуры тех же организаций.

Образцы шпионских программ, заблокированные на компьютерах АСУ в первом полугодии 2021 года, по количеству атакованных машин и количеству дней, прошедших с момента первого обнаружения каждого образца



Хотя эти «аномальные» атаки шпионских программ и не являются масштабными, они составляют непропорционально большую долю всех атак шпионских программ.

Например, в Азии почти каждый шестой компьютер из числа атакованных шпионскими программами, был на самом деле атакован одним из «аномальных» образцов (2,1% из 11,9%, как показано на графике ниже).

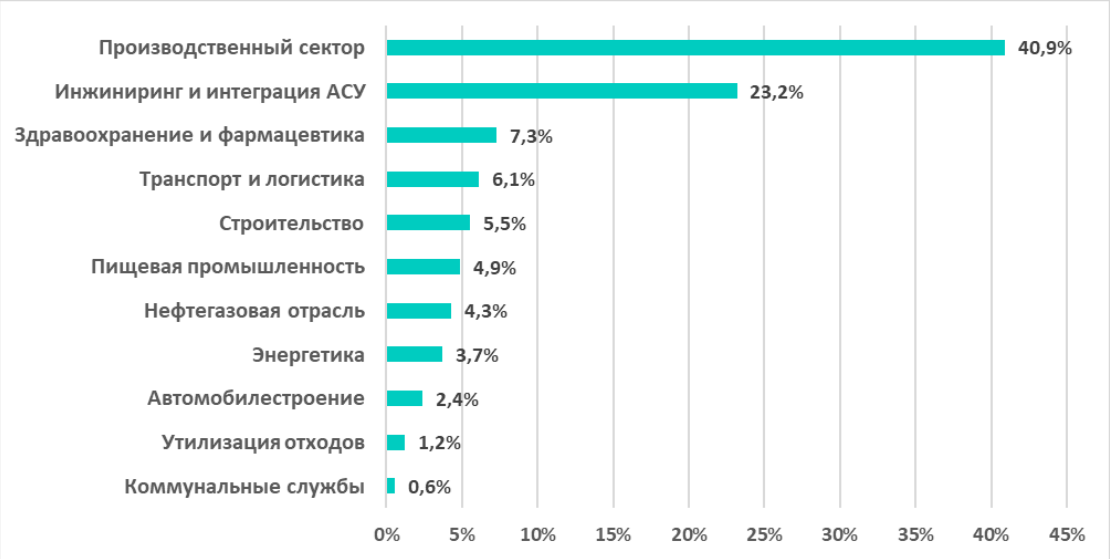
В Африке (2% из 15,4%), на Ближнем Востоке (1,3% из 10,1%), Европе (0,7% из 6,3%), России (0,7% из 6,8%), Австралии и Новой Зеландии (0,6% из 5,6%) и в Северной Америке (0,5% из 3,3%) приблизительно каждая десятая атака с использованием шпионских программ была «аномальной».

Похоже, что в экосистеме атак коммерческих шпионских программ возник новый быстро развивающийся кластер, где сокращается масштаб атак и ограничивается использование каждого образца вредоносных программ за счет быстрой замены новым образцом.

Процент компьютеров АСУ, на которых было заблокировано шпионское ПО в первом полугодии 2021 года. Все шпионские программы по сравнению с «аномальными» образцами

Примечательно, что большинство компьютеров АСУ, на которых в первом полугодии 2021 года были заблокированы атаки «аномальных» образцов шпионских программ, использовались в сфере производства, а также инжиниринга и интеграции АСУ. Такой перекос в имеющихся данных предположительно связан с характером этих атак, более подробную информацию о котором можно найти в разделе «Инфраструктура сбора данных» данного отчета.

Распределение по отраслям компьютеров АСУ, на которых были заблокированы «аномальные» шпионские программы в первом полугодии 2021



Анализ шпионских программ

Если говорить об образцах шпионских программ, использованных в «аномальных» атаках на компьютеры АСУ в первом полугодии 2021 года, то это — всё те же распространённые Agent Tesla (Origin Logger), HawkEye, Noon (Formbook), Masslogger, Snake Keylogger, Azorult, Lokibot и иже с ними.

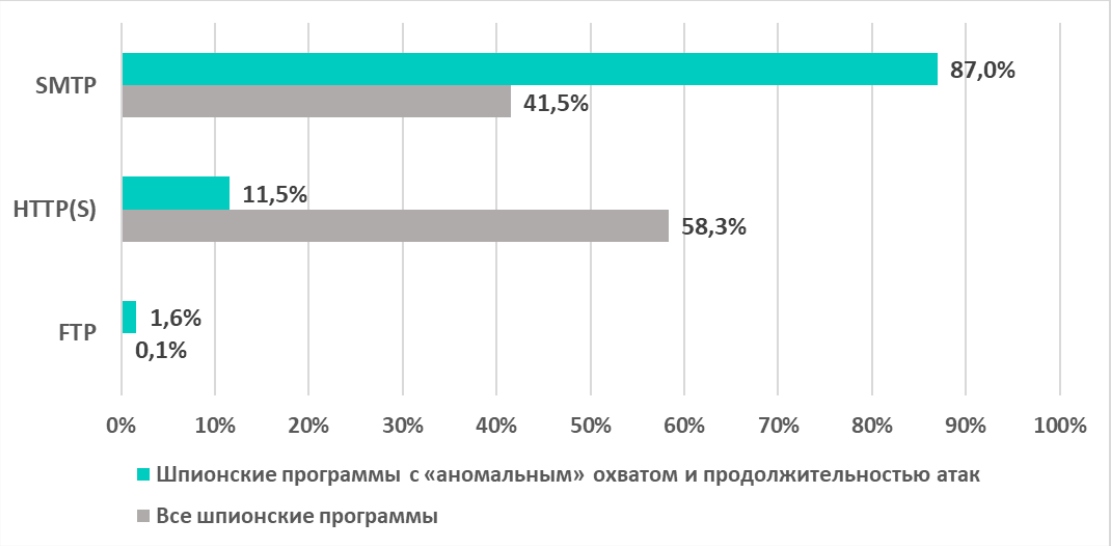
Как правило, заблокированные образцы были многократно обфусцированы так, что слои обфускации были вложены один внутрь другого — как матрешки. При этом двоичный код скрывается в ресурсах приложения. Одна из популярных реализаций заключается в хранении вредоносного кода в байтах изображения с использованием цветовой схемы RGBA (красный, зеленый, синий и альфа каналы).

Единственное существенное различие, которое нам удалось обнаружить между обычными образцами шпионских программ и образцами из «аномальных» атак, — это тип инфраструктуры, используемой для сбора украденных данных.

Инфраструктура сбора данных

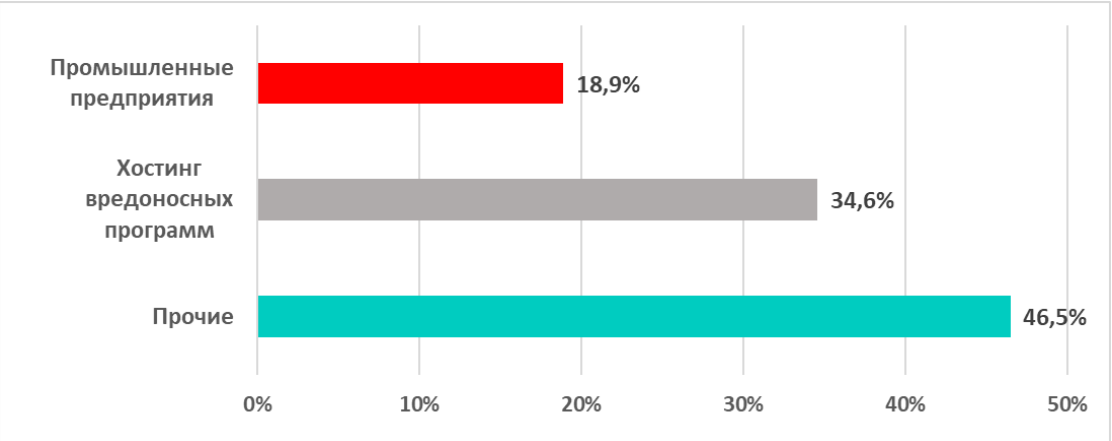
В отличие от обычных шпионских программ конфигурация большинства образцов, использованных в «аномальных» атаках, предусматривала работу с «командными» серверами, использующими протокол SMTP (а не FTP или HTTP(s)) для организации одностороннего канала связи. Это означает, что целью злоумышленников была исключительно кража данных, без возможности передачи команд от сервера клиенту.

Распределение образцов шпионских программ по протоколу управления, обычное шпионское ПО и образцы, использованные в «аномальных» атаках



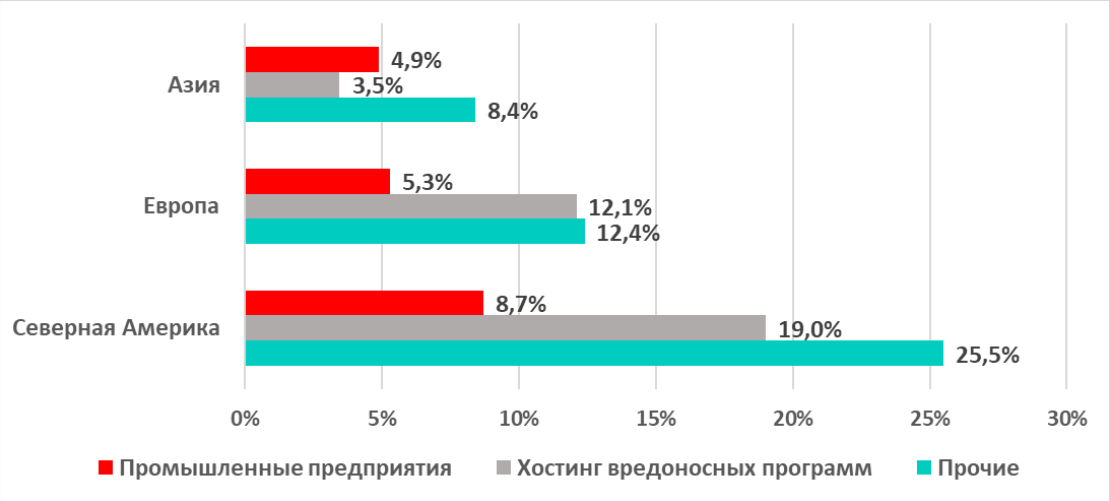
Около 18,9% «аномальных» образцов шпионских программ было сконфигурировано для подключения к почтовым серверам, принадлежащим промышленным предприятиям, которые ранее стали жертвами их атак.

Распределение образцов шпионских программ, использованных в «аномальных» атаках, по типу размещения почтовых серверов сбора украденных данных



Почти все серверы сбора украденных данных (99,8%), обнаруженные в конфигурации образцов шпионских программ, использованных в «аномальных» атаках, развернуты в трех регионах: Азии, Европе и Северной Америке.

Распределение образцов шпионских программ, использованных в «аномальных» атаках, по регионам и по способам размещения инфраструктуры серверов сбора украденных данных (SMTP). ТОП-3 регионов



Мы также обнаружили, что большинство серверов сбора украденных данных, включая принадлежащие промышленным компаниям, размещены в Северной Америке.

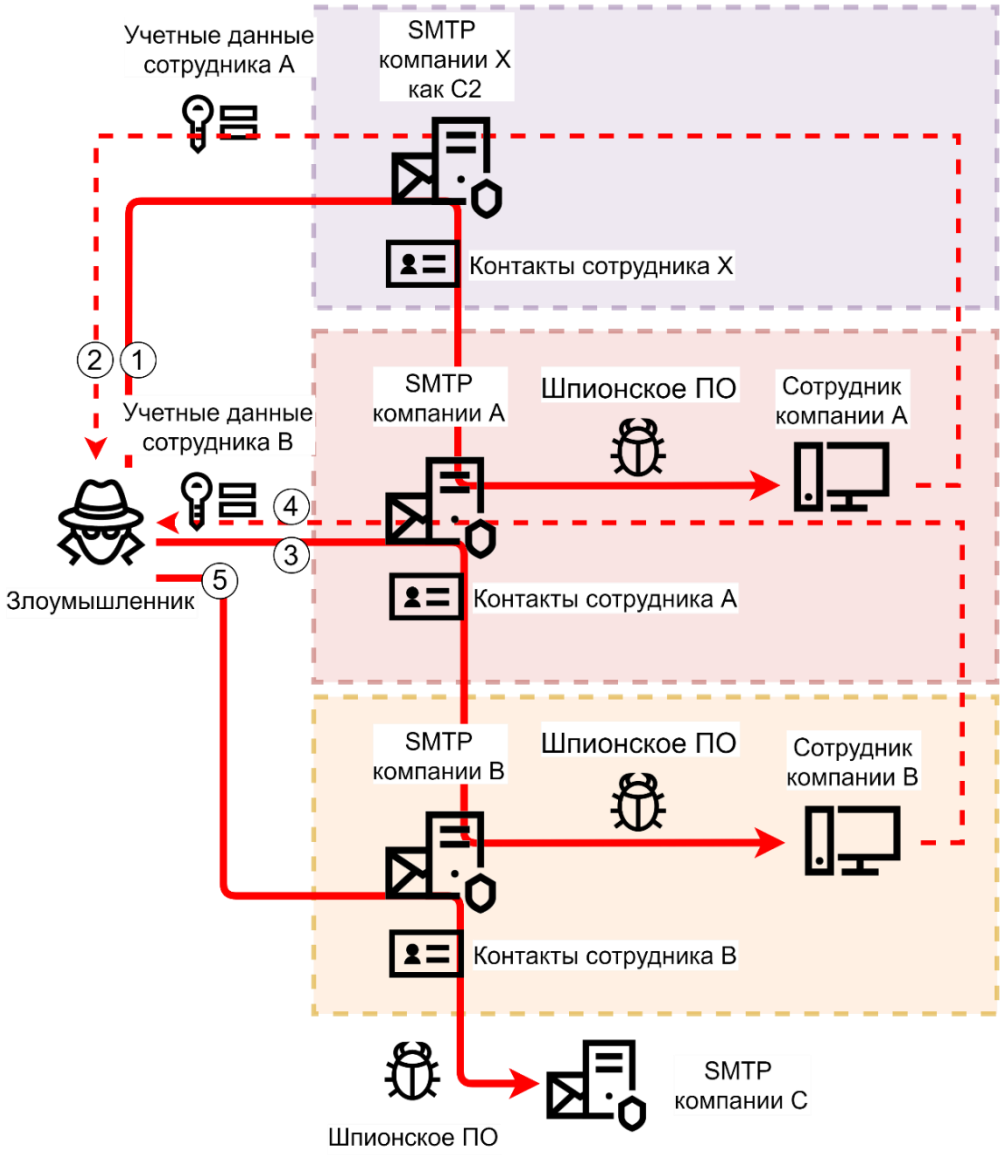
Это неожиданный результат, поскольку 34,6% атакованных компьютеров АСУ принадлежат азиатским компаниям. Однако по результатам анализа выяснилось, что неожиданно большое количество азиатских промышленных компаний среднего размера размещает свою публичную инфраструктуру (DNS-серверы, корпоративные веб-серверы и почтовые серверы) не в Азии, а в Америке — на серверах, арендованных либо непосредственно у американских провайдеров, либо у азиатских провайдеров-посредников, фактически предоставляющих доступ к инфраструктуре американских провайдеров.

Тактика, методы и процедуры

Мы полагаем, что на начальном этапе украденные данные используются злоумышленниками в первую очередь для распространения атаки в локальной сети организации (посредством фишинговых писем) и для атаки на другие организации с целью сбора дополнительных учетных данных.

Анализ адресов отправителей и получателей в фишинговых электронных письмах, отправленных злоумышленниками, и адресов вновь обнаруживаемых командных серверов показал, что значительный процент украденных почтовых аккаунтов впоследствии используется как для распространения атаки со взломанных систем промышленного предприятия (на организации, являющиеся его деловыми партнерами и контрагентами), так и в качестве серверов сбора украденных данных. Эта тактика показана на схеме ниже.

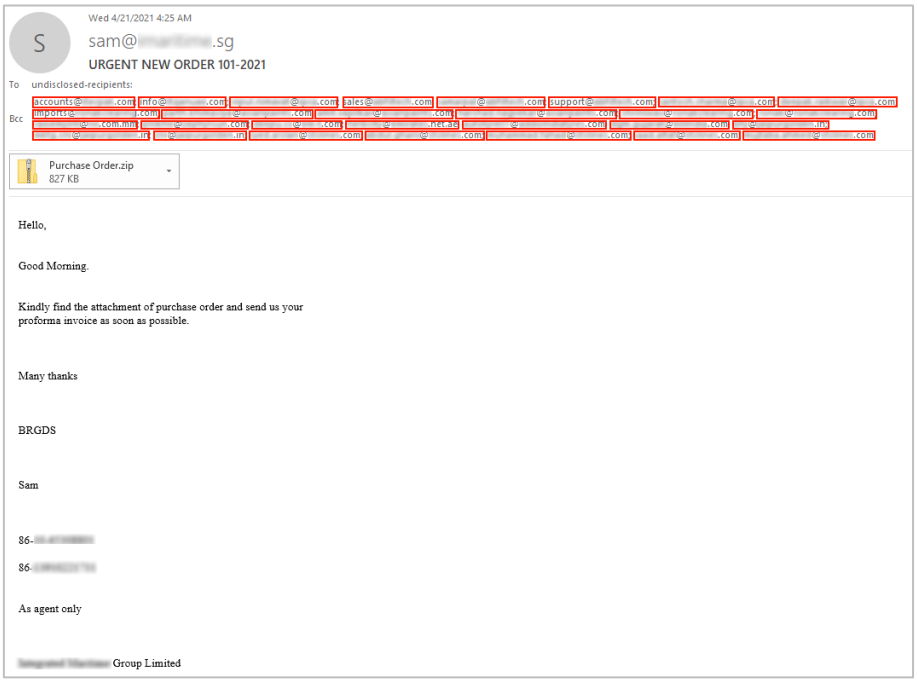
Сбор и использование учетных данных злоумышленниками



Ниже показан пример фишингового электронного письма, отправленного злоумышленниками с использованием украденных учетных данных (учетной записи электронной почты) пользователя. Электронное письмо было отправлено через почтовый сервер атакованной организации от имени пользователя, чей почтовый аккаунт был взломан. Адресатами фишингового письма (и, соответственно, объектами атаки) в данном случае были 28 пользователей из 7 промышленных компаний.

В целом в рамках этого исследования было выявлено более 2 000 взломанных (т. е. использованных шпионскими программами в качестве серверов сбора украденных данных) учетных записей электронной почты, принадлежащих промышленным компаниям. По нашим оценкам, общее количество учетных записей электронной почты, украденных в результате этих атак, превышает 7 000.

Электронное письмо, отправленное в рамках атаки, распространявшейся по списку контактов взломанной учетной записи



Wed 4/21/2021 4:25 AM

sam@[redacted].sg

URGENT NEW ORDER 101-2021

To undisclosed-recipients:

Bcc accounts@[redacted].com info@[redacted].com sales@[redacted].com support@[redacted].com imports@[redacted].com

Purchase Order.zip
827 KB

Hello,

Good Morning.

Kindly find the attachment of purchase order and send us your proforma invoice as soon as possible.

Many thanks

BRGDS

Sam

86-[redacted]

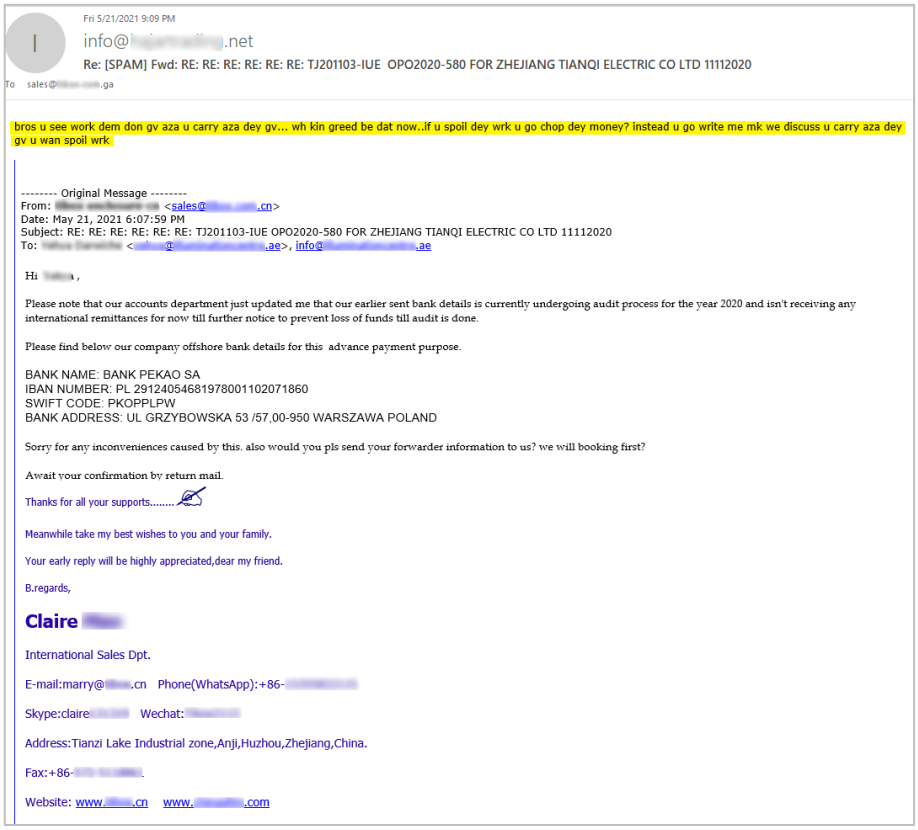
86-[redacted]

As agent only

[redacted] Group Limited

Некоторые злоумышленники на следующем этапе атаки применяли технику Business Email Compromise, — анализа деловой переписки и последующего мошенничества методами социальной инженерии с целью подмены данных банковских транзакций. Пример электронных писем, используемых в таких атаках, приведен ниже.

Мошенническое электронное письмо, отправленное в рамках атаки типа Business Email Compromise



Fri 5/21/2021 9:09 PM

info@[redacted].net

Re: [SPAM] Fwd: RE: RE: RE: RE: RE: RE: TJ201103-IUE OPO2020-580 FOR ZHEJIANG TIANQI ELECTRIC CO LTD 11112020

To sales@[redacted].ga

bros u see work dem don gv aza u carry aza dey gv... wh kin greed be dat now..if u spoil dey wrk u go chop dey money? instead u go write me mk we discuss u carry aza dey gv u wan spoil wrk

-------- Original Message --------
From: [redacted] <sales@[redacted].cn>
Date: May 21, 2021 6:07:59 PM
Subject: RE: RE: RE: RE: RE: RE: TJ201103-IUE OPO2020-580 FOR ZHEJIANG TIANQI ELECTRIC CO LTD 11112020
To: [redacted] <[redacted].ae>, info@[redacted].ae

Hi [redacted],

Please note that our accounts department just updated me that our earlier sent bank details is currently undergoing audit process for the year 2020 and isn't receiving any international remittances for now till further notice to prevent loss of funds till audit is done.

Please find below our company offshore bank details for this advance payment purpose.

BANK NAME: BANK PEKAO SA
IBAN NUMBER: PL 29124054681978001102071860
SWIFT CODE: PKOPPLPW
BANK ADDRESS: UL GRZYBOWSKA 53 /57,00-950 WARSZAWA POLAND

Sorry for any inconveniences caused by this. also would you pls send your forwarder information to us? we will booking first?

Await your confirmation by return mail.

Thanks for all your supports.....

Meanwhile take my best wishes to you and your family.

Your early reply will be highly appreciated,dear my friend.

B.regards,

Claire [redacted]

International Sales Dpt.

E-mail:marry@[redacted].cn Phone(WhatsApp):+86-[redacted]

Skype:claire[redacted] Wechat:[redacted]

Address:Tianzi Lake Industrial zone,Anji,Huzhou,Zhejiang,China.

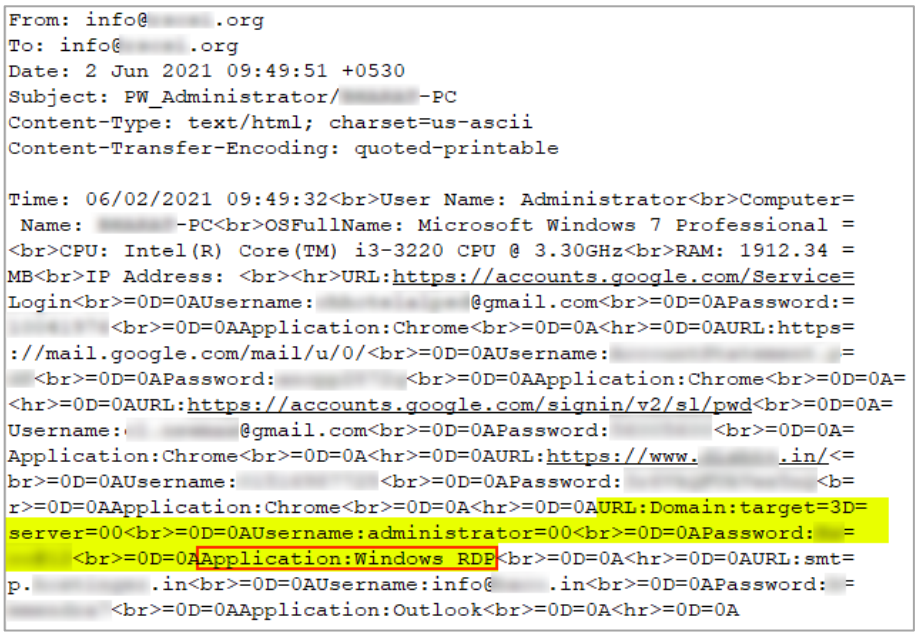
Fax:+86-[redacted].

Website: www.[redacted].cn www.[redacted].com

Другие злоумышленники специализируются на краже учетных данных для последующей продажи. Их интересуют, в частности:

- Учетные данные персональных финансовых сервисов: онлайн-банкинга, платежных кошельков, криптобирж и т.п.
- Учетные данные социальных сетей и других общедоступных интернет-сервисов.
- Учетные данные для доступа к корпоративным сетевым сервисам (SMTP, SSH, RDP, VPN и др.).

Электронное письмо, в котором шпионская программа пересылает злоумышленникам украденные учетные данные для доступа по RDP

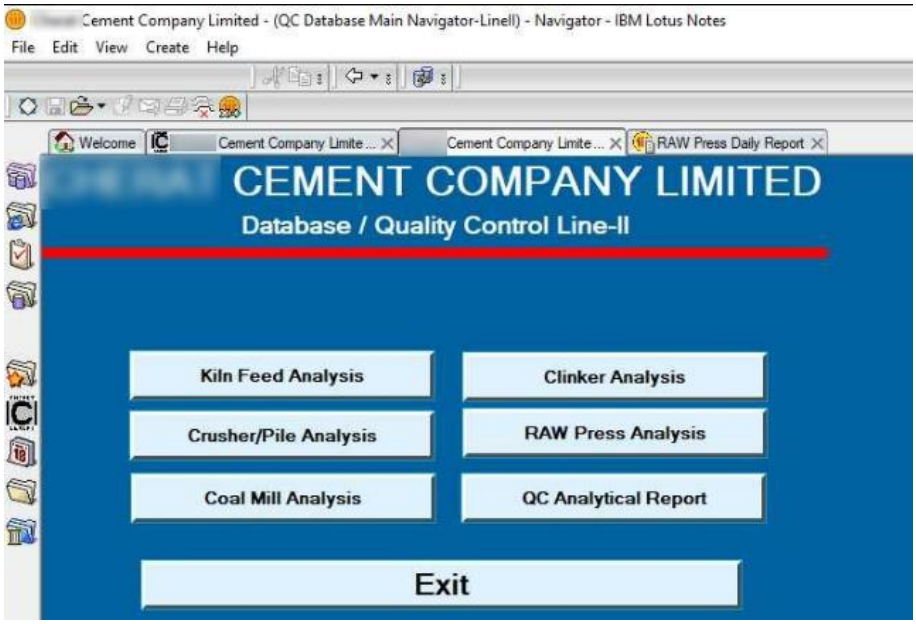


```
From: info@[redacted].org
To: info@[redacted].org
Date: 2 Jun 2021 09:49:51 +0530
Subject: PW_Administrator/[redacted]-PC
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Time: 06/02/2021 09:49:32<br>User Name: Administrator<br>Computer=
 Name: [redacted]-PC<br>OSFullName: Microsoft Windows 7 Professional =
<br>CPU: Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz<br>RAM: 1912.34 =
MB<br>IP Address: <br><hr>URL:https://accounts.google.com/Service=
Login<br>=0D=0AUsername: [redacted]@gmail.com<br>=0D=0APassword:=
[redacted]<br>=0D=0AApplication:Chrome<br>=0D=0A<hr>=0D=0AURL:https=
://mail.google.com/mail/u/0/<br>=0D=0AUsername: [redacted]=
[redacted]<br>=0D=0APassword: [redacted]<br>=0D=0AApplication:Chrome<br>=0D=0A=
<hr>=0D=0AURL:https://accounts.google.com/signin/v2/sl/pwd<br>=0D=0A=
Username: [redacted]@gmail.com<br>=0D=0APassword: [redacted]<br>=0D=0A=
Application:Chrome<br>=0D=0A<hr>=0D=0AURL:https://www.[redacted].in/<=
br>=0D=0AUsername: [redacted]<br>=0D=0APassword: [redacted]<b=
r>=0D=0AApplication:Chrome<br>=0D=0A<hr>=0D=0AURL:Domain:target=3D=
server=00<br>=0D=0AUsername:administrator=00<br>=0D=0APassword: [redacted]=
[redacted]<br>=0D=0AApplication:Windows RDP<br>=0D=0A<hr>=0D=0AURL:smt=
p.[redacted].in<br>=0D=0AUsername:info@[redacted].in<br>=0D=0APassword: [redacted]=
[redacted]<br>=0D=0AApplication:Outlook<br>=0D=0A<hr>=0D=0A
```

Основываясь на снимках экрана, сделанных шпионскими программами, и на других косвенных уликах, можно отметить, что некоторые злоумышленники проявляют особый интерес к промышленным компаниям и их инфраструктуре. Такой интерес объясняется значительной разницей в цене на разные типы учетных записей на торговых интернет-площадках (см. ниже).

Снимок экрана, сделанный шпионской программой



На данном этапе исследования выявленная ранее «аномалия» получает логическое объяснение: обнаруженные «аномальные» образцы так ограниченны по охвату и имеют такой короткий срок службы по той причине, что злоумышленники генерируют уникальные образцы (с конкретной конфигурацией сервера сбора украденных данных) для каждой фишинговой рассылки. Сгенерированные образцы обычно отправляются лишь части адресов из списка контактов жертвы, атакованной на предыдущем этапе.

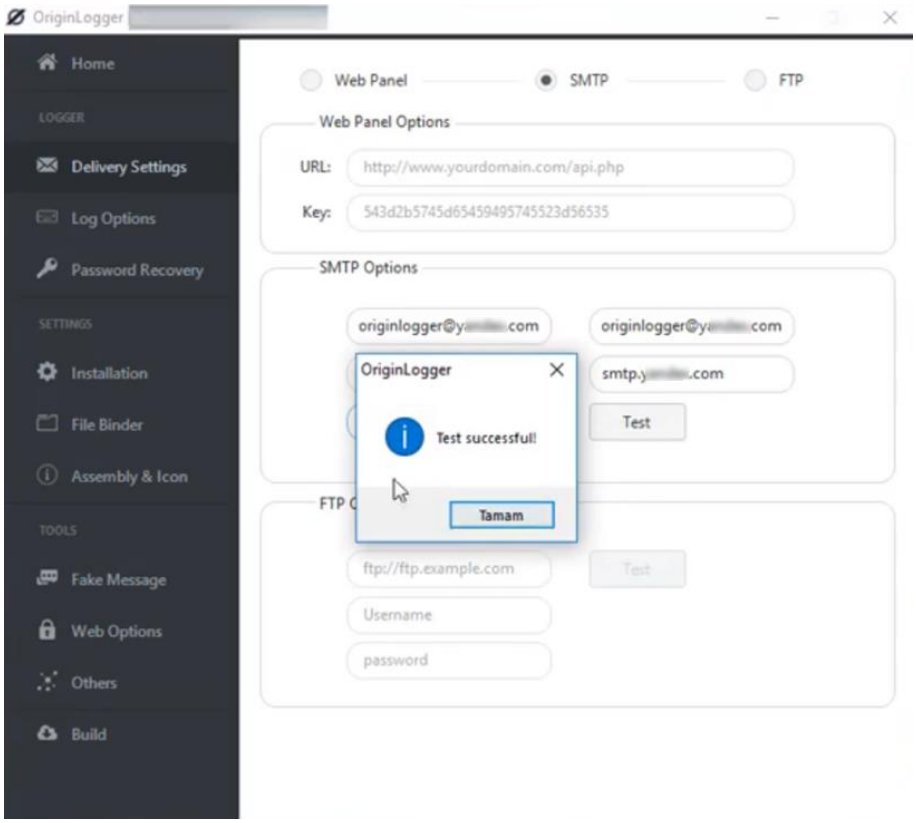
Когда взломанная учетная запись электронной почты используется для передачи данных с атакованного компьютера на сервер, поток писем, содержащих украденные данные в машинно-читаемом формате, обычно обнаруживается антиспам-решением, и письма перемещаются в папку для спама, где в большинстве случаев остаются незамеченными до момента очистки папки.

Организаторы атак

Анализ данных, проведенный в рамках исследования «аномальных» атак с использованием шпионских программ, пролил некоторый свет на общую ситуацию с кампаниями по краже учетных данных, проводимыми сотнями независимых злоумышленников.

Многие средства сборки шпионских программ имеют функцию проверки доступности командного сервера на этапе конфигурации. Если для этих целей используется почтовый сервер, они отправляют тестовое сообщение и затем проверяют его доставку, подключившись к серверу с аккаунтом адресата.

Скриншот инструмента OriginLogger после успешного тестирования на доступность конфигурации сервера сбора данных, использующего протокол SMTP



Ниже, на скриншоте тестового сообщения, отправленного средством сборки шпионской программы на сервер сбора данных, видно, что подобные сообщения могут содержать полезные сведения об инфраструктуре, используемой злоумышленниками: поле темы тестового сообщения содержит имя пользователя, имя компьютера и IP-адрес машины, с которой было отправлено сообщение.

Тестовое электронное письмо, отправленное на сервер сбора данных для его верификации

```
From: am                3          .com
To: am                  @          .com
Date: 23 Mar 2021 23:51:28 +0100
Subject: DELL/DELL-PC  IP: 129.20
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Test successful!
```

Другие исследователи выявили, что некоторые средства сборки могут также отправлять определенные данные разработчикам средств сборки вредоносных программ. Это означает, что разработчики могут использовать эти функции для слежки за своими клиентами. Другие средства сборки, отправляющие злоумышленникам «приветственные» электронные письма, например HawkEye, не содержат существенной информации об их пользователях.

Тестовое сообщение с приветствием от HawkEye

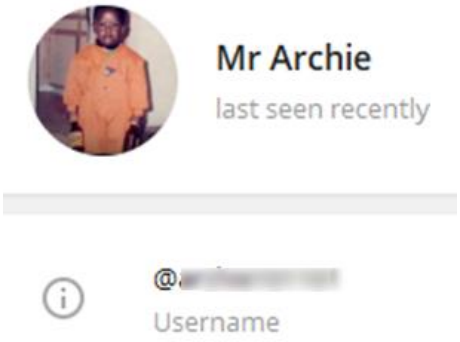
```
From: info@[redacted].org
To: info@[redacted].org
Date: 25 Mar 2021 22:07:45 +0100
Subject: HawkEye Keylogger - Test Email 3/25/2021 10:07:41 PM
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Dear HawkEye Customer!=0D=0A=0D=0ALet us informed you that your e=
-mail is working properply and has now been verified by HawkEye K=
eylogger. You may proceed now.=0D=0A=0D=0ABest Regards=0D=0AAdmin
```

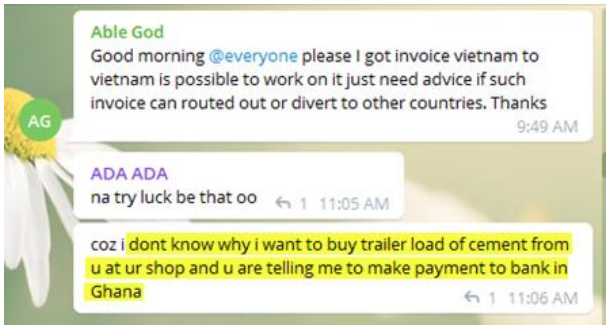
Анализ информации об операторах «аномальных» атак с использованием шпионского ПО (утечку которой они, скорее всего, допустили при тестировании вредоносных программ на компьютерах, используемых ими для повседневной деятельности) позволил нам больше узнать об их тактиках, техниках и процедурах, бэкенд-инфраструктуре , используемой при подготовке атак, а также о различных используемых сервисах. В том числе, для в аренды инфраструктуры, взаимодействии с другими киберпреступниками и сбыта краденных данных.

Этот анализ также показал, что многие злоумышленники могут иметь отношение к африканским странам.

Учетная запись Telegram, принадлежащая организатору атак, который входит также во многие другие аналогичные группы



Скриншот чата, в котором организаторы атак обсуждают атаки типа Business Email Compromise



IP-адреса хостов, используемых организаторами атак в составе инфраструктуры бэкенд-серверов, перечислены в «Приложении I — Индикаторы компрометации».

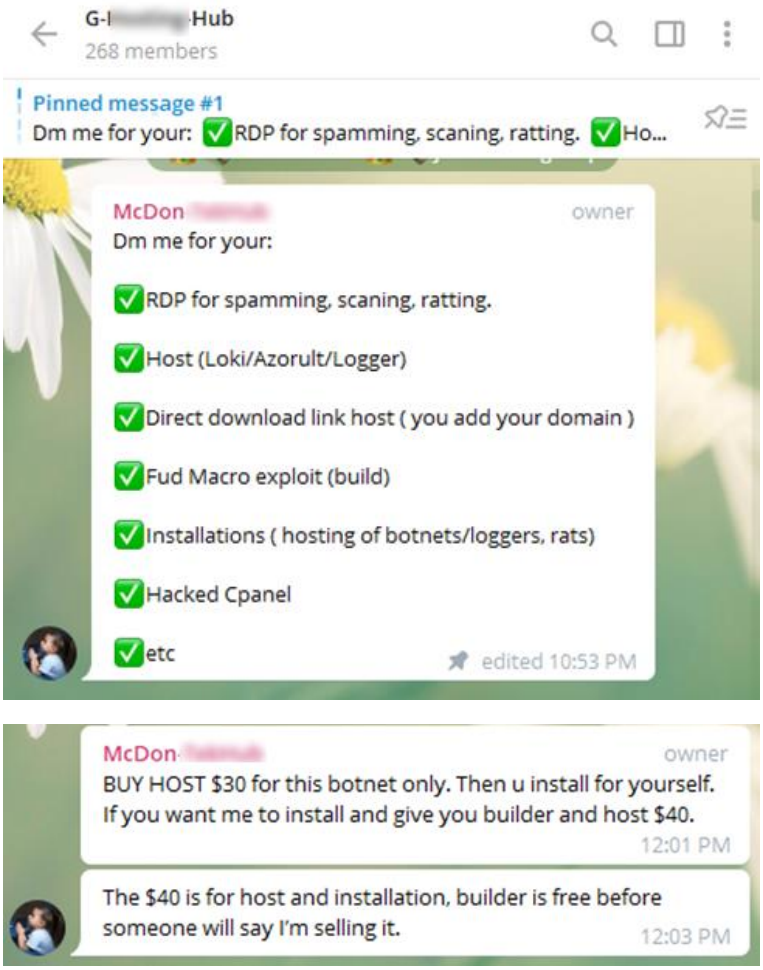
Разработчики вредоносного ПО и поставщики услуг по схеме «Шпионское ПО как сервис»

За последние 5 лет, с тех пор как был опубликован исходный код некоторых популярных шпионских программ, он стал широко использоваться по схеме "вредоносное ПО как услуга" (Malware-as-a-Service, MaaS) — в интернет-магазинах стали продавать лицензии на средства сборки вредоносных программ, а не на сами вредоносные программы как продукт.

Скриншот сайта, на котором продается инструмент OriginLogger (он же Agensla)

Иногда разработчики вредоносных программ продают не средство сборки, а доступ к инфраструктуре, заранее настроенной для сборки вредоносных программ, и параллельно рекламируют дополнительные услуги.

Скриншоты чата в Telegram с предложением продавца шпионских программ



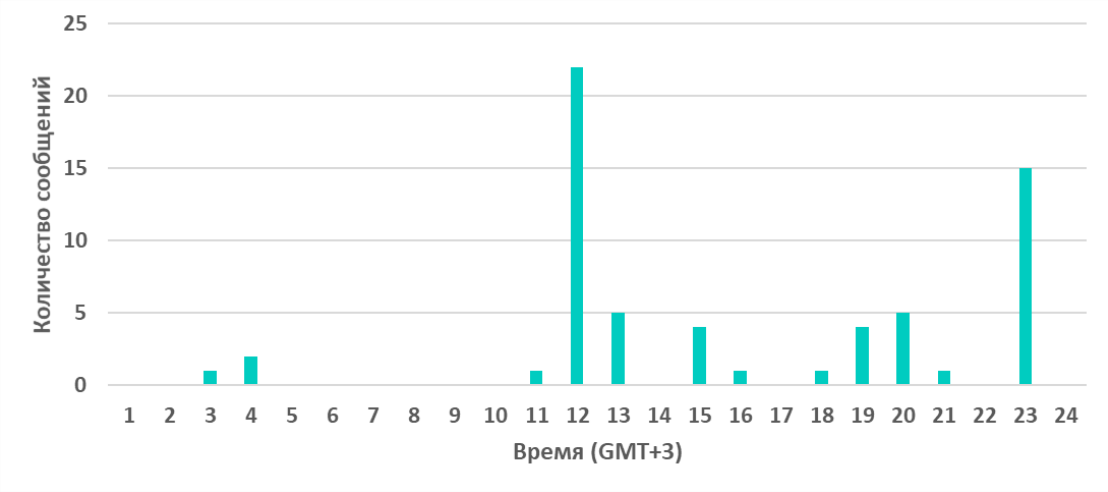
Многие разработчики шпионских программ предлагают свои продукты в социальных сетях, форумах и чатах и даже записывают видеоуроки. Мы проанализировали доступные источники информации, опубликованной многими разработчиками вредоносных программ (продавцами средства сборки шпионских программ). В рамках этого исследования нам удалось отследить создание и распространение экземпляров шпионского ПО, примененных в «аномальных» атаках: от операторов атак до используемой ими инфраструктуры MaaS и связанных с ней провайдеров и разработчиков. Дальнейший анализ социальных сетей, чатов и форумов, на которых общаются операторы и разработчики, показал, что значительная часть независимых разработчиков вредоносного ПО и лиц, предоставляющих услуги по его использованию, вероятно, говорит на русском (т. е. они могут иметь отношение к странам постсоветского пространства) и турецком языках.

Это наблюдение основано на нескольких фактах:

- Предполагаемый часовой пояс — исходя из времени суток, когда разработчики вредоносных программ активны в чатах и форумах.

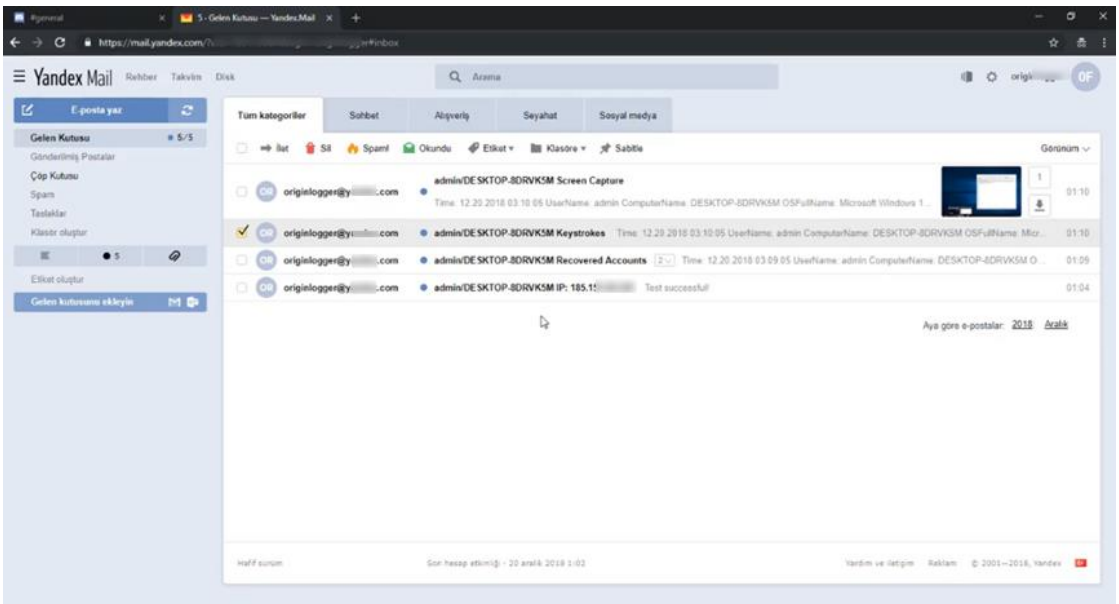
- Предполагаемые региональные/языковые параметры на основе скриншотов, видео и сообщений разработчиков вредоносных программ.

Пример анализа часового пояса на основе активности разработчика вредоносных программ в чате



Другой пример — видеоурок, записанный продавцом инструмента OriginLogger. На видео виден интерфейс его почтового ящика на Яндексе на турецком языке. Кроме того, автор не совсем корректно использовал эффект размытия на видео и не полностью скрыл данные, собранные демонстрируемой шпионской программой. Анализ веб-адресов, собранных шпионской программой и отображаемых в веб-браузере создателя видеоурока, показывает, что у автора есть учетные записи на турецких форумах и даже в одном из турецких университетов.

Скриншот видеоурока, записанного продавцом OriginLogger



Скриншоты видеоурока, записанного продавцом OriginLogger, в котором неправильно используется эффект размытия

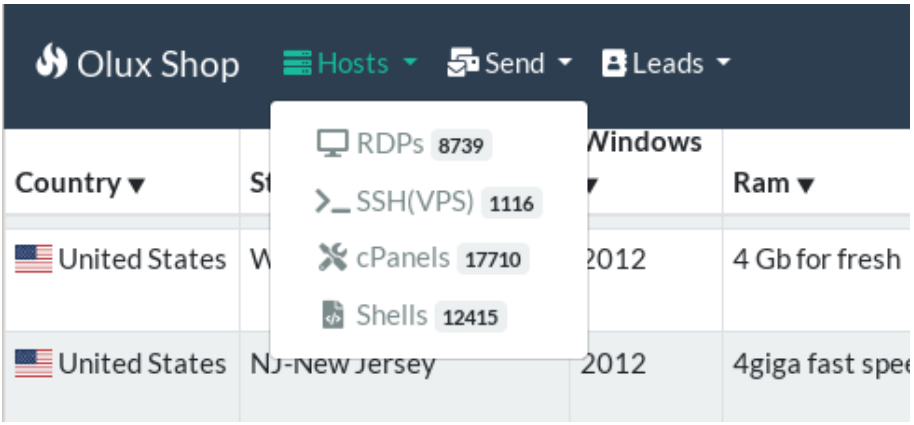
Торговые площадки

Данные об операторах атак позволяют получить определенные сведения об используемых ими сервисах по предоставлению вредоносных программ (а также о разработчиках вредоносных программ и провайдерах соответствующих услуг). Кроме того, эти данные проливают свет на один из способов монетизации атак по сбору учетных данных. Им оказалась продажа украденных учетных данных на различных торговых площадках.

Анализ используемых злоумышленниками сервисов и торговых площадок показал, что кампании по сбору учетных данных являются одним из составных элементов огромного конвейера различных вредоносных сервисов, от разработки вредоносных программ и связанной с ней инфраструктуры до торговых платформ, предлагающих доступ к широкому спектру корпоративных сетей.

В ходе данного исследования было выявлено более 25 различных торговых площадок, на которых продавались данные, украденные в ходе расследованных нами кампаний по сбору учетных данных промышленных предприятий. На этих торговых площадках различные продавцы предлагают тысячи аккаунтов RDP, SMTP, SSH, cPanel и учетных записей электронной почты, а также вредоносные программы, мошеннические схемы и образцы электронных писем и веб-страниц для применения социальной инженерии.

Интернет-страница торговой площадки, на которой продается более 8000 учетных записей RDP



По результатам анализа предложений и цен можно отметить следующую тенденцию: доступ к корпоративным сетям промышленных предприятий (посредством RDP, SSH, SMTP и другими способами) стоит в 8-10 раз дороже, чем доступ к инфраструктурам облачного хостинга, таким как AWS, DigitalOcean, Azure и прочим.

Анализ всего портфеля учетных записей, предлагаемых продавцом, может показать, что он специализируется на определенных типах аккаунтов. В частности, некоторые продавцы предлагают в основном учетные записи корпоративных сетей (в том числе сетей промышленных компаний).

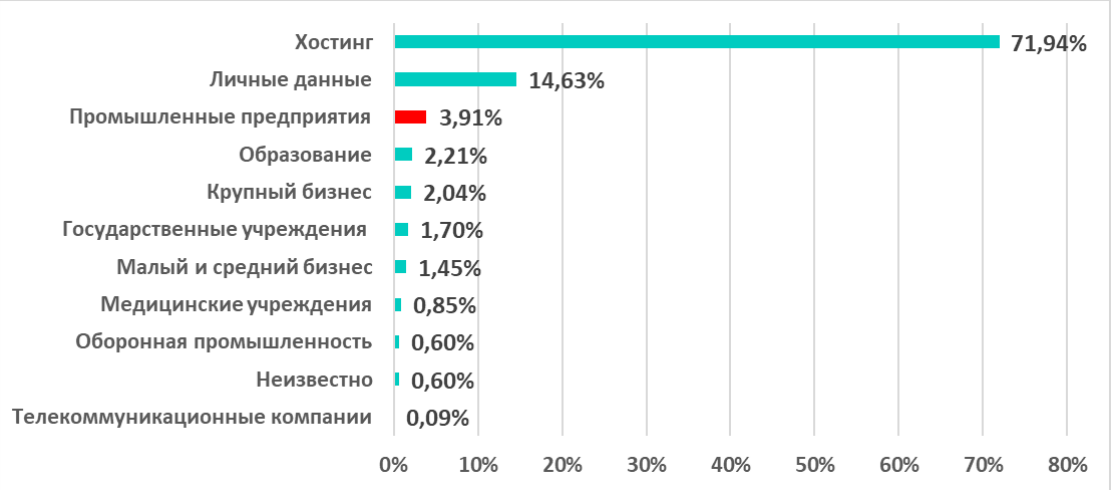
Предложения RDP-доступа к сетям некоторых промышленных компаний

Olux Shop Hosts Send Leads Tickets 0.00 My Account

Country	State	Windows	Ram	Access	Username	Detected Hosting	Seller	Price	Added on	Buy
United States	TN-Tennessee	2019	12GB RDP LONGTIME STRONG	ADMIN	Ad**	[redacted] Chemical Company	seller156	80	07/08/2021 05:39:22 am	Buy
United States	TN-Tennessee	2019	32GB RDP LONGTIME AND STRON...	ADMIN	Ad**	[redacted] Chemical Company	seller156	80	07/08/2021 06:08:08 am	Buy
United States	TN-Tennessee	2019	12GB RDP LONGTIME STRONG	ADMIN	Ad**	[redacted] Chemical Company	seller156	80	07/08/2021 05:39:22 am	Buy
United States	TN-Tennessee	2016	16GB RDP LONGTIME AND STRON...	ADMIN	Ad**	[redacted] Chemical Company	seller163	80	07/08/2021 06:30:33 am	Buy
United States	TN-Tennessee	2016	16GB RDP LONGTIME AND STRON...	ADMIN	Ad**	[redacted] Chemical Company	seller163	80	07/08/2021 06:30:34 am	Buy
United States	TN-Tennessee	2016	16GB RDP LONGTIME AND STRON...	ADMIN	Ad**	[redacted] Chemical Company	seller163	80	07/08/2021 06:30:34 am	Buy
United States	IN-Indiana	2019	16GB RDP LONGTIME AND STRONG	ADMIN	Ad**	[redacted] Company	seller156	80	07/08/2021 05:57:30 am	Buy
United States	IN-Indiana	2016	10GB RDP LONGTIME AND STRONGER	ADMIN	Ad**	[redacted] Company	seller163	80	07/08/2021 06:21:54 am	Buy
India	MP-Madhya Pradesh	2012	4GB H@cked - Strong - FAST	ADMIN	ad**	[redacted] Private Limited	seller127	13	07/04/2021 11:21:39 pm	Buy
United States	CA-California	2019	10GB RDP LONGTIME STRONG	ADMIN	Ad**	Energy [redacted]	seller156	80	07/08/2021 05:47:06 am	Buy

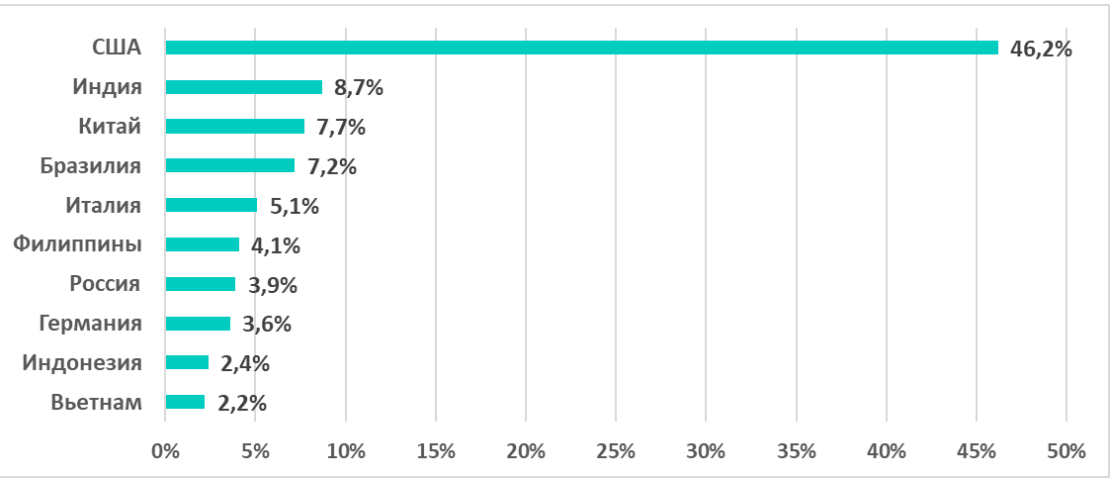
Статистический анализ метаданных более чем 50 000 взломанных учетных записей RDP, продаваемых на торговых площадках, показывает, что 1954 учетных записи (3,9%) принадлежат промышленным предприятиям.

Взломанные учетные записи RDP, продаваемые на торговых площадках, по типам



Статистика взломанных учетных записей RDP промышленных предприятий в разбивке по странам показывает, что более 46% учетных записей, продаваемых на торговых площадках, принадлежит компаниям из США, а остальные — компаниям из Азии, Европы и Латинской Америки.

Взломанные учетные записи RDP, продаваемые на торговых площадках, по странам, ТОП-10



Заключение

Меры безопасности и контроля, которые активно принимаются в информационной и технологической инфраструктуре по всему миру, вынуждают киберпреступников развиваться. Одним из отмеченных нами изменений в подходах злоумышленников стал переход от массовых атак к ограниченным по охвату и очень краткосрочным (как с точки зрения инфраструктуры сбора украденных данных, так и в плане срока службы используемых вредоносных образцов) сериям атак. Еще одна применяемая тактика — распространение этих атак изнутри инфраструктуры компании-жертвы, что позволяет «легитимизировать» фишинговый почтовый трафик. Использование легальных почтовых ящиков (взломанных на предыдущем этапе атаки) позволяет злоумышленникам быстро сменять инфраструктуру для сбора данных, сводя к минимуму обнаружение своей активности решениями сетевой безопасности.

Подобные атаки являются весьма существенной проблемой — в частности, в первой половине 2021 года, в зависимости от региона, до одной шестой части всех компьютеров, подвергавшихся атакам шпионского ПО, было атаковано именно с применением этой тактики.

Согласно данным нашей телеметрии, серверы более чем 2 000 промышленных предприятий во всем мире были использованы в качестве инфраструктуры сбора украденных данных и распространения вредоносного ПО. Злоумышленники использовали списки контактов и адреса деловых партнеров атакованных промышленных предприятий для дальнейшего распространения атаки. По нашим оценкам, коэффициент конверсии украденных почтовых аккаунтов в серверы сбора данных составляет примерно 1/4. Как минимум 7 000 корпоративных учетных записей было украдено киберпреступниками в исследованных атаках.

Есть много способов нелегитимного использования украденных данных аутентификации, в том числе наиболее опасными субъектами, такими как группы злоумышленников, специализирующихся на программах-вымогателях и APT. Как показывает анализ торговых площадок в интернете, наибольшим спросом пользуются учетные данные, обеспечивающие доступ к внутренним системам предприятий. Предложение, по-видимому, соответствует спросу: в ходе исследования на торговых площадках нами было обнаружено почти 2 000 учетных записей RDP для промышленных предприятий.

Рекомендации

Рекомендуется принять следующие меры для обеспечения надлежащей защиты промышленного предприятия, его партнерской сети и бизнеса в целом:

- Рассмотрите возможность внедрения двухфакторной аутентификации для доступа к корпоративной электронной почте и другим интернет-сервисам (включая RDP, шлюзы VPN-SSL и прочее), которые могли бы использоваться злоумышленниками для получения доступа к внутренней инфраструктуре компании, критически важным данным и системам.
- Убедитесь, что все устройства в офисной и технологической сетях защищены современным решением для обеспечения безопасности конечных устройств, которое корректно настроено и регулярно обновляется.
- Регулярно проводите обучение сотрудников безопасной работе с входящей электронной почтой и защите от вредоносных программ, которые могут содержаться во вложениях в электронные письма.
- Регулярно проверяйте папки со спамом, а не просто очищайте их.
- Регулярно проверяйте, не продаются ли учетные записи вашей организации
- Рассмотрите возможность использования технологий sandbox для автоматической проверки вложений во входящих электронных письмах. Убедитесь, что она настроена так, чтобы не пропускать сообщения из «доверенных» источников, включая компании-партнеры и организации из списка контактов. Никто не защищен от взлома на 100%.
- Проверяйте вложения в исходящих сообщениях электронной почты. Это может помочь определить, не скомпрометированы ли учетные записи ваших сотрудников.

Приложение I — Индикаторы компрометации

IP-адреса инфраструктуры операторов атак

105.112.101.7	105.112.145.6	105.112.37.193
105.112.102.213	105.112.147.156	105.112.37.222
105.112.107.100	105.112.147.20	105.112.38.173
105.112.109.252	105.112.148.252	105.112.38.201
105.112.113.164	105.112.148.60	105.112.38.218
105.112.113.250	105.112.150.35	105.112.38.249
105.112.114.120	105.112.178.164	105.112.39.130
105.112.115.230	105.112.26.202	105.112.39.167
105.112.115.4	105.112.32.44	105.112.41.0
105.112.117.199	105.112.33.155	105.112.41.149
105.112.121.59	105.112.33.233	105.112.46.233
105.112.144.173	105.112.33.40	105.112.46.38
105.112.144.56	105.112.35.117	105.112.50.73
105.112.144.77	105.112.37.192	105.112.50.80

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com