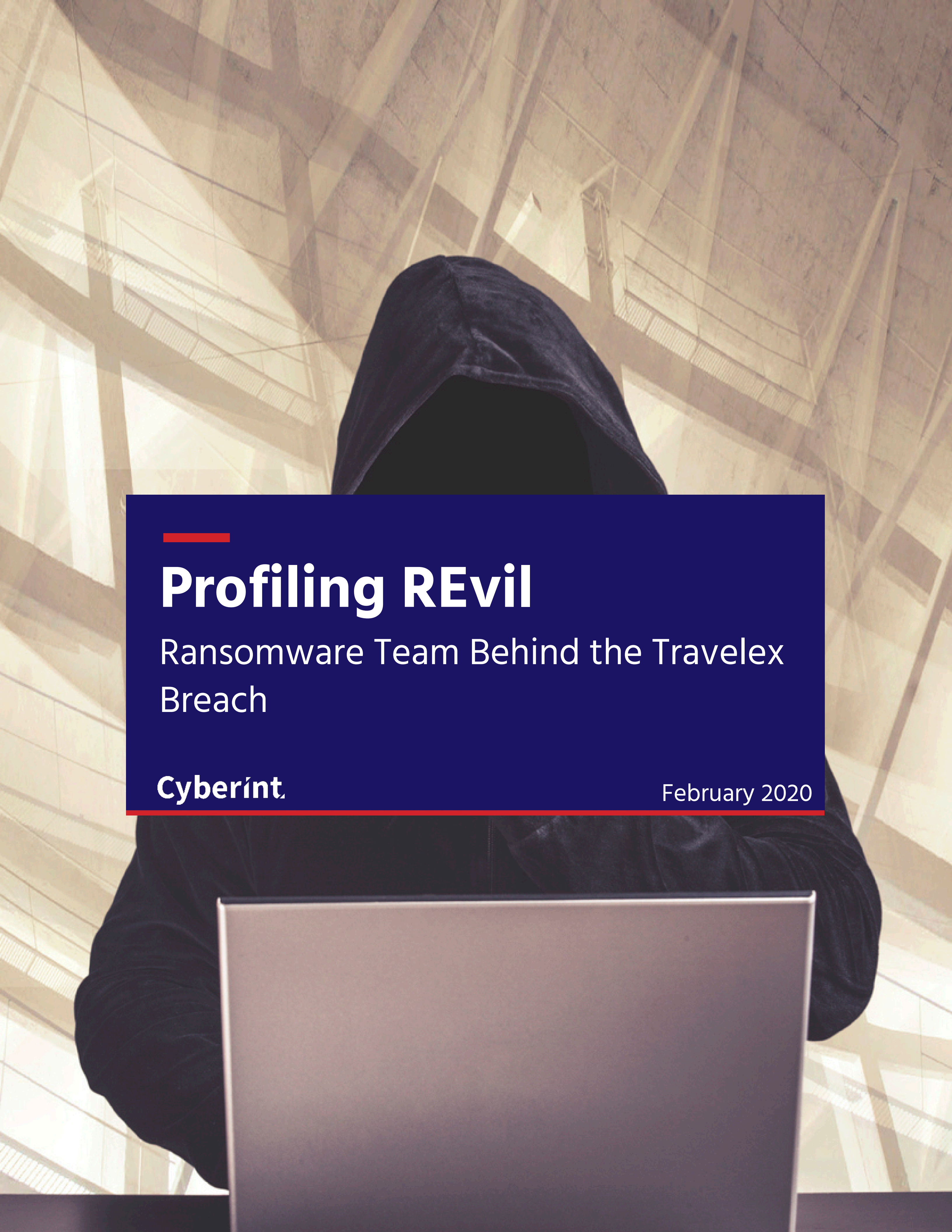


Profiling REvil

Ransomware Team Behind the Travelex Breach

Cyberint

February 2020

Table of Contents

Executive Summary

Targeted ransomware attacks appear to be on the increase thus far in 2020 with a new major incident seemingly being reported each week.

This ‘steal, encrypt and leak’ tactic appears to have started in November 2019 with the ‘Maze Crew’, operators of the Maze Ransomware-as-a-Service (RaaS). Following their lead, those behind the ‘REvil/Sodinokibi’, ‘Nemty’ and ‘DoppelPaymer’ ransomware threats have adopted similar approaches, threating to leak stolen data if ransoms aren’t paid, to increase the success of their financially motivated campaigns.

This report by provides insights into "REvil Ransomware Team" - the one most notably mentioned in connection with Travelex ransomware attack in early January 2020. It covers the team's recent activities, its reputation on the cybercriminal forums, its own affiliate program and more.

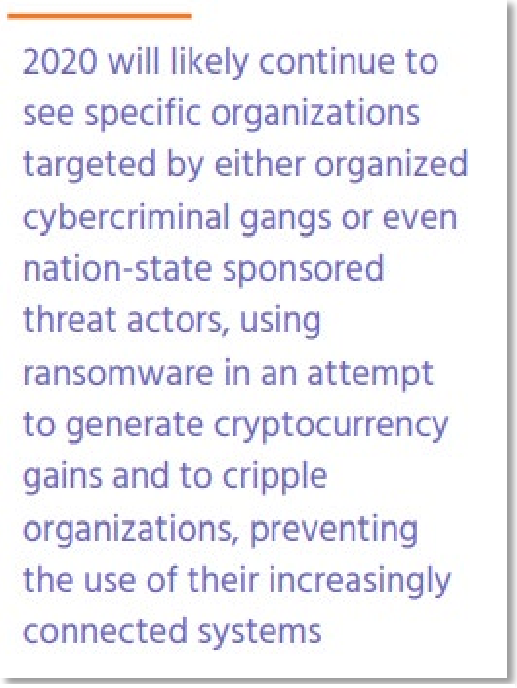
Whilst little is known about the true identities of those behind the personas ‘UNKN’ and ‘unknown’, likely one and the same person, or the members of the ‘REvil Ransomware Team’, insights into their activity obtained by monitoring their posts on cybercriminal forums reveal the threat actors are Russian-speaking and are likely based in, or from, the Commonwealth of Independent States (CIS). Furthermore, they are undoubtedly experienced in the execution of a RaaS operation, with capabilities to develop enhancements to the ransomware and manage a seemingly successful affiliate program.

Whilst the true scale of REvil’s victims cannot be fully assessed, especially as some may pay for restoration and to protect their anonymity, two organizations have been identified as paying to recover from their REvil ransomware attacks: Albany International Airport and PerCSoft, a US-based provider of cloud services.

Background

Consistent with CyberInt's research team predictions provided in *CiPulse 2020 Threat Landscape Report*[1] (Figure 1), targeted ransomware attacks appear to be on the increase thus far in 2020, with a new major incident seemingly being reported each week.

Of the high profile ransomware incidents seen so far this year, it appears that the cybercriminal groups responsible have adopted similar tactics, techniques and procedures (TTP), targeting large organizations and attempting to extort high value ransoms through the compromise of the target network, theft of valuable data and, finally, the encryption of data and systems.



2020 will likely continue to see specific organizations targeted by either organized cybercriminal gangs or even nation-state sponsored threat actors, using ransomware in an attempt to generate cryptocurrency gains and to cripple organizations, preventing the use of their increasingly connected systems

Figure 1 - CyberInt CiPulse 2020 Threat Landscape Report

Unlike traditional ransomware attacks, often delivered via indiscriminate mass-mailing campaigns delivering ransomware components to unwitting individuals, these incidents demonstrate an organized effort that compromises the networks of often large and multinational organizations utilizing various offensive techniques and exploits. Post-compromise, this 'double-pronged' attack, in which the victim's data is stolen prior to its encryption, applies additional pressure to pay the ransom - otherwise the stolen data is resold or leaked on cybercriminal forums.

Of the data observed as being leaked by these threat groups thus far, files relating to the organization's IT infrastructure are often selected as these provide useful intelligence, and in some cases credentials, that can be abused by other threat actors.

The threat of confidential data being leaked may coerce many into paying the ransom to prevent data exposure that could lead to the incident becoming public knowledge with the associated reputational loss, even when the organization might otherwise be able to recover from the ransomware attack itself. Surely, those tempted to pay are placing their trust in those that stole the data in the first place and there is no guarantee that it won't be leaked and/or abused at a later date.

[1] https://l.cyberint.com/cipulse-2020-threat-landscape-report

This ‘steal, encrypt and leak’ tactic appeared to have started in November 2019 with the ‘Maze Crew’, operators of the Maze Ransomware-as-a-Service (RaaS), publishing data stolen from Allied Universal[2], a US-headquartered security and facility services company, following the expiry of the ransom payment deadline.

Following this lead, those behind the ‘REvil/Sodinokibi’, ‘Nemty’ and ‘DoppelPaymer’ ransomware threats have adopted similar approaches, threating to leak stolen data if ransoms aren’t paid, to increase the success of their financially motivated campaigns.

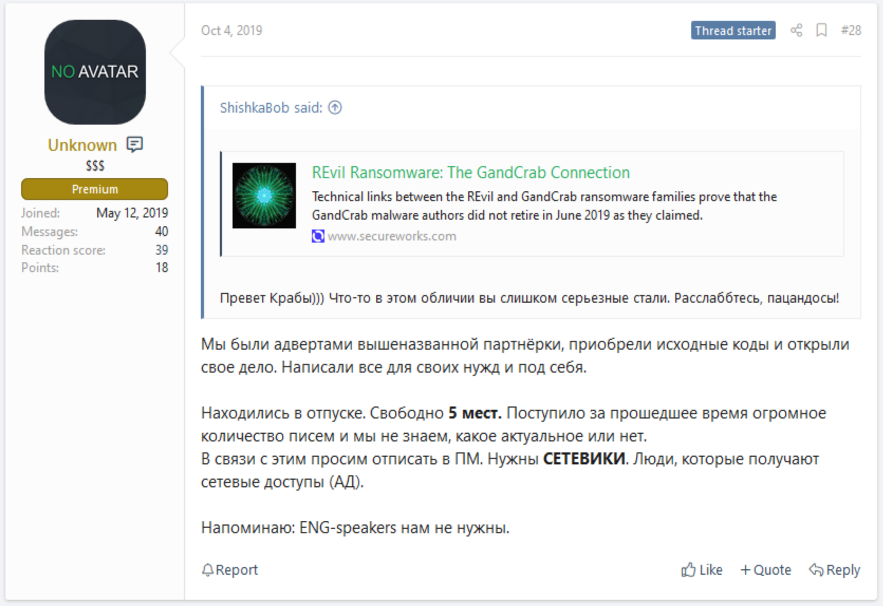
Although there have been numerous notable examples of ransomware incidents thus far in 2020, this report focuses on the cybercriminal group known as ‘REvil Ransomware Team’, also known as ‘Sodin’ and ‘Sodinokibi’, who were responsible for the major ransomware incident experienced by Travelex over the New Year period. Whilst CyberInt, and others, have previously published reports providing details of the ransomware’s technical capabilities, this report seeks to provide an overview of the threat actors themselves, their modus operandi and a summary of their activity in 2020 thus far.

[2] https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

REvil Ransomware

Also known as ‘Sodin’ and ‘Sodinokibi’, REvil is a ransomware-as-a-service (RaaS) threat that was first observed in April 2019[3] and rose to prominence following the retirement of the Gandcrab RaaS on May 31, 2019 after reportedly earning it’s operators in excess of US$2 billion since January 2018.

Subsequent research by Secureworks’ Counter Threat Unit (CTU) published in September 2019[4] identified technical links between REvil and GandCrab, suggesting that the developers shifted to a new ransomware variant. Responding to this article, a spokesperson or potential leader of the ‘REvil Ransomware Team’, known as ‘Unknown’ (on ‘XSS’ forum) and ‘Unkn’ (on ‘Exploit’ forum), posted on the XSS cybercriminal forum that they were previously ‘adverts’ (адвертами) of the GandCrab affiliate program and have acquired the source code to launch their own RaaS business (Figure 2).



Joined: May 12, 2019
Messages: 40
Reaction score: 39
Points: 18

Oct 4, 2019 Thread starter #28

ShishkaBob said:

REvil Ransomware: The GandCrab Connection
Technical links between the REvil and GandCrab ransomware families prove that the GandCrab malware authors did not retire in June 2019 as they claimed.
www.secureworks.com

Превет Крабы))) Что-то в этом обличии вы слишком серьезные стали. Расслаббтесь, пацандосы!

Мы были адвертами вышеназванной партнёрки, приобрели исходные коды и открыли свое дело. Написали все для своих нужд и под себя.

Находились в отпуске. Свободно **5 мест.** Поступило за прошедшее время огромное количество писем и мы не знаем, какое актуальное или нет.
В связи с этим просим отписать в ПМ. Нужны **СЕТЕВИКИ**. Люди, которые получают сетевые доступы (АД).

Напоминаю: ENG-speakers нам не нужны.

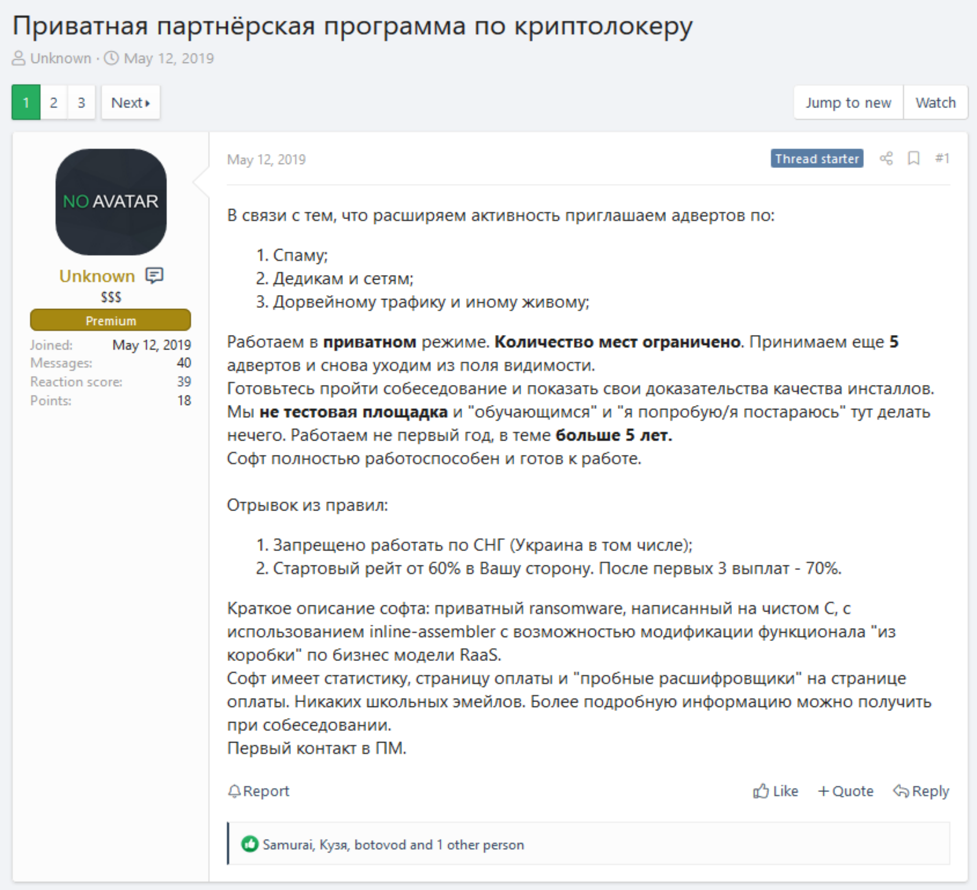
Figure 2 - ‘Unknown’ response to the REvil/GandCrab link

Furthermore, this spokesperson states that GandCrab “*wrote everything for their needs and for themselves*”, perhaps hinting as to why their ransomware threat has included new features that would improve its appearance to would-be affiliates.

[3] https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

[4] https://www.secureworks.com/blog/revil-the-gandcrab-connection

Providing further insight into the ransomware's construction, affiliate recruitment forum posts (Figure 3) describe REvil as being *"private ransomware written in pure C, using inline-assembler with the ability to modify the functionality"*, additionally the posts suggest that the control panel, used to manage ransomware campaigns, provides statistics along with the payment page and trial decryptors (likely to provide reassurance to victims prior to making payment).



Приватная партнёрская программа по криптолокеру

Unknown · May 12, 2019

Joined:	May 12, 2019
Messages:	40
Reaction score:	39
Points:	18

May 12, 2019

В связи с тем, что расширяем активность приглашаем адвертов по:

1. Спаму;
2. Дедикам и сетям;
3. Дорвейному трафику и иному живому;

Работаем в **приватном** режиме. **Количество мест ограничено**. Принимаем еще **5** адвертов и снова уходим из поля видимости.
Готовьтесь пройти собеседование и показать свои доказательства качества инсталлов.
Мы **не тестовая площадка** и "обучающимся" и "я попробую/я постараюсь" тут делать нечего. Работаем не первый год, в теме **больше 5 лет.**
Софт полностью работоспособен и готов к работе.

Отрывок из правил:

1. Запрещено работать по СНГ (Украина в том числе);
2. Стартовый рейт от 60% в Вашу сторону. После первых 3 выплат - 70%.

Краткое описание софта: приватный ransomware, написанный на чистом C, с использованием inline-assembler с возможностью модификации функционала "из коробки" по бизнес модели RaaS.
Софт имеет статистику, страницу оплаты и "пробные расшифровщики" на странице оплаты. Никаких школьных эмейлов. Более подробную информацию можно получить при собеседовании.
Первый контакт в ПМ.

Samurai, Кузя, botovod and 1 other person

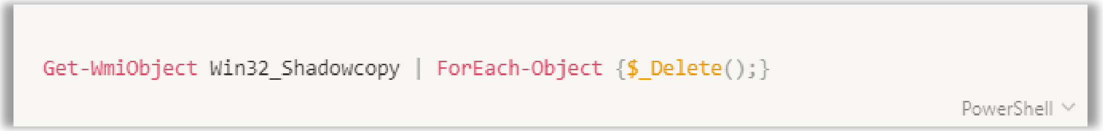
Figure 3 - Affiliate advertisement providing an overview of REvil's construction

Subsequent forum posts also hint at other REvil capabilities, many of which have been documented by various security researchers following analysis of the binaries, including:

- Local Privilege Escalation (LPE) through the exploition of CVE-2018-8453 (Win32k Elevation of Privilege Vulnerability)[5] for both 32-bit and 64-bit versions of Windows
- Windows User Access Control (UAC) bypass

[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8453

- PowerShell and regular expression support, the former being used to delete Windows Volume Shadow Copies to thwart restoration attempts:



```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_Delete();}
```

Figure 4 - PowerShell used to delete Windows Volume Shadow Copies

- Detection of the default and system languages along with keyboard layouts to prevent the encryption of machines in 'friendly' countries (the targeting of CIS countries is prohibited by the group's rules)
- Future developments, as of May 2019, were to improve network and RDP functionality although this may relate to how initial network intrusions are performed rather specific exploit capabilities be included within the ransomware itself.

As previously reported, the ransomware includes an encoded JSON configuration file within itself that is decoded upon execution. This configuration, in addition to suspected affiliate and campaign identifiers likely used to allow REvil to track the use of their RaaS and manage their 'cut', contains a number of keys and values (Table 1) that define how the ransomware interacts with the victim system.

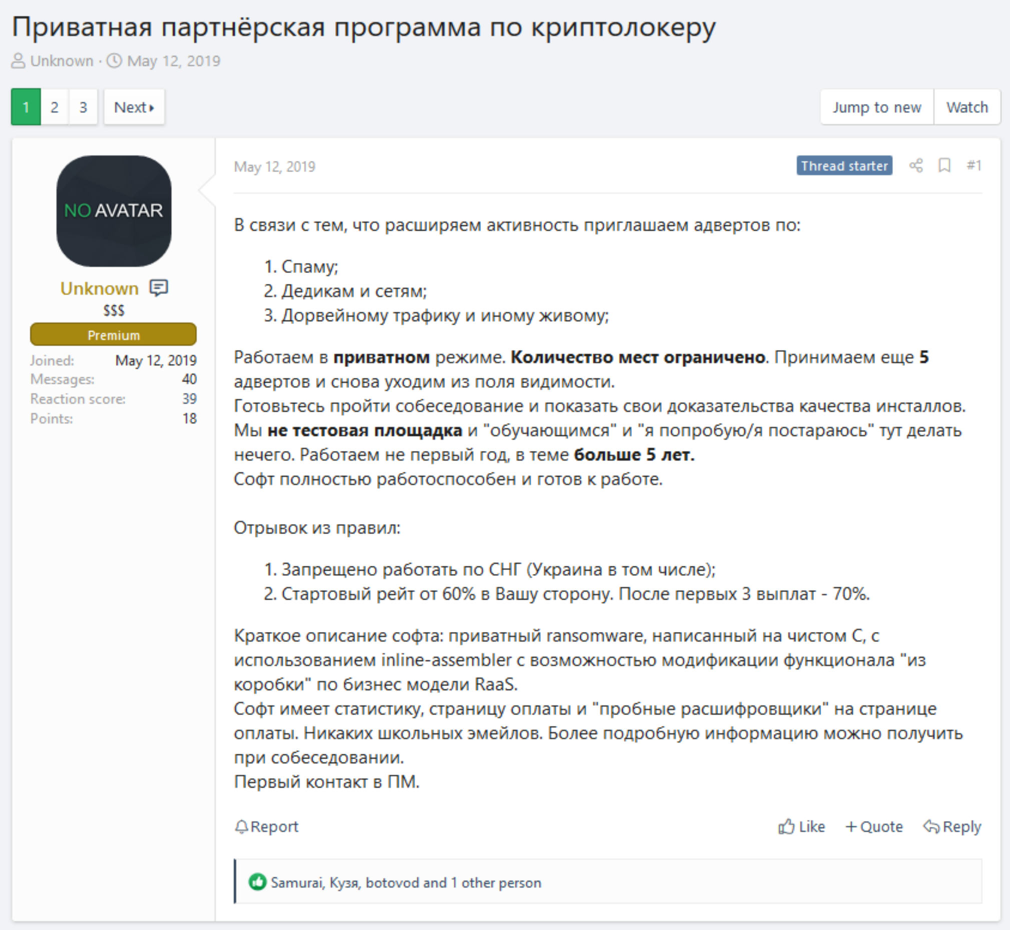
Configuration Values

Key	Value	Notes
pk	<Base64>	Public Key used for file encryption
pid	[0-9]{2}	Potential affiliate or campaign ID
sub	[0-9]{3}	Potential affiliate or campaign ID
dbg	(True|False)	Debug/development switch
fast	(True|False)	Determines how large files are encrypted (fast = partial encryption)
wipe	(True|False)	Determines if directories listed in the 'wfld' key are deleted; Reportedly removed in later versions;
wht		Whitelist
wht > fld	<string>	Whitelisted directories
wht > fls	<string>	Whitelisted files
wht > ext	<string>	Whitelisted file extensions
wfld	<string>	Wipe folders, for deletion
prc	<string>	Processes to terminate to allow the encryption of their data
dmn	<string>	C2 domains
net	(True|False)	Exfiltrate host/malware information to C2 domain
nbody	<base64>	Encoded ransom note
nname	<EXT>-readme.txt	Ransom note filename prefixed by the encrypted file extension (a random string generated at execution and appended to encrypted files)
exp	(True|False)	Exploit local privilege escalation (LPE) vulnerability
img	<base64>	Ransom text added to background image, directing used to find the ransom note file
arn	(True|False)	Reportedly present since 6 Oct 2019; Configures persistence in the Registry 'run' key

Table 1 - REvil Ransomware Configuration Keys/Values

REvil Affiliate Program

For those looking to become involved with REvil, posts on both the ‘Exploit’ and ‘XSS’ Russian-speaking cybercriminal forums, the earliest of which appears to be May 12, 2019, invite applications from those interested in participating in a ‘Private Crypto Locker Affiliate Program’ (Figure 5).



Приватная партнёрская программа по криптолокеру

Unknown · May 12, 2019

Joined: May 12, 2019
Messages: 40
Reaction score: 39
Points: 18

May 12, 2019 Thread starter #1

В связи с тем, что расширяем активность приглашаем адвертов по:

1. Спаму;
2. Дедикам и сетям;
3. Дорвейному трафику и иному живому;

Работаем в **приватном** режиме. **Количество мест ограничено**. Принимаем еще **5** адвертов и снова уходим из поля видимости.
Готовьтесь пройти собеседование и показать свои доказательства качества инсталлов.
Мы **не тестовая площадка** и "обучающимся" и "я попробую/я постараюсь" тут делать нечего. Работаем не первый год, в теме **больше 5 лет.**
Софт полностью работоспособен и готов к работе.

Отрывок из правил:

1. Запрещено работать по СНГ (Украина в том числе);
2. Стартовый рейт от 60% в Вашу сторону. После первых 3 выплат - 70%.

Краткое описание софта: приватный ransomware, написанный на чистом C, с использованием inline-assembler с возможностью модификации функционала "из коробки" по бизнес модели RaaS.
Софт имеет статистику, страницу оплаты и "пробные расшифровщики" на странице оплаты. Никаких школьных эмейлов. Более подробную информацию можно получить при собеседовании.
Первый контакт в ПМ.

Samurai, Кузя, botovod and 1 other person

Figure 5 - Private Crypto Locker Affiliate Program post

Rather than allowing anyone to join the program the group only appears to be interested in those with particular skillsets, inviting ‘serious and experienced professionals’ to demonstrate evidence of the ‘quality of their installations’ in a private interview process.

This process itself is conducted without the use of names via private messages, preferably using a specified Russian-language Jabber platform, and, should the applicant be successful, technical detail of the ransomware including screenshots would be shared.

Successful applicants will also need to adhere to the group's rules, namely it is forbidden from operating in CIS countries, including the Ukraine, (albeit the ransomware has checks to detect and prevent the encryption of CIS language machines) and the initial affiliate income is 60%, increasing to 70% after the first three successful payments. Considering the high ransoms demanded thus far, such as the US$6 million reportedly demanded in the Travelex incident, even when shared these 'cuts' could see both parties making millions of dollars per high profile attack.

Unfortunately, or not, those that are new to the scene ("*обучающимся*" - learners and "*я попробую/я постараюсь*" I will try/I will try) are advised that there is no place for them and English-speakers are specifically excluded from applying. The latter exclusion making reference to the investigative journalist Brian Krebs no doubt due to his work in exposing and reporting on cybercriminal groups.

Likely maintaining exclusivity on their RaaS platform, REvil periodically open slots for new affiliate applications and over time have been more specific in their requirements and expectations, presumably as the group focused more on higher value targets such as corporate networks rather than individual end-users.

Affiliate Invitations

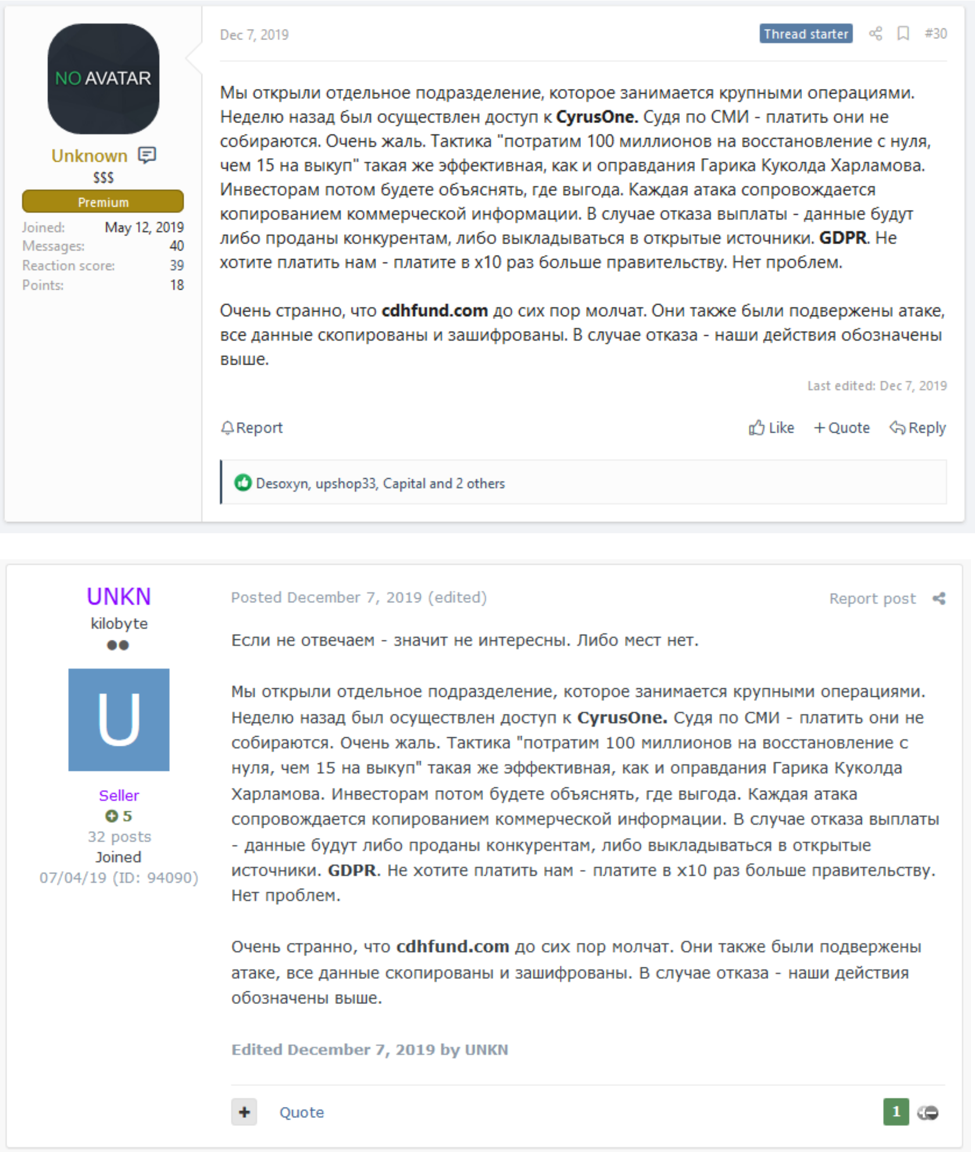
Forum Post Date	Slots Available	Comments
May 20, 2019	4	
May 27, 2019		'dediks, spammers and those who [compromise] networks'
June 17, 2019	2	'Any deposit is possible - up to 1,000,000USD'
June 19, 2019	0	
July 3, 2019	4	'Delete 2 more, 4 places available'
July 4, 2019		'Limited number of seats'
July 12, 2019		'Interested in associates that can provide systematic access rather than one time 5-10 networks'
July 17, 2019	5	'In a week about 5 places will be vacated'
July 27, 2019		'All places occupied, except for networks and Dediks. Spammers and door-keepers are temporarily not accepted.'
August 8, 2019	3	'Places for networks/dedikov'
October 4, 2019	5	'Gain network access (AD)'
October 10, 2019	2	'Still available'
October 18, 2019	1	Applicants with 100 'dediks' a day or network-level access
January 7, 2020	0	
January 11, 2020	1	
January 12, 2020	3	'take major RDP players as well as targeted attacks'
January 22, 2020	0	
January 27, 2020	3	

Table 2 - Affiliate vacancy posts since May 2019

Whilst it is not clear if the number of affiliates increases overtime or if vacancies arise as others are removed from the service, the forum posts over the past year appear to demonstrate increasing capabilities by limiting applicants to those that can compromise networks, including Windows Active Directory domains, gain access to Remote Desktop Protocol (RDP) hosts and perform targeted attacks.

The requirement for affiliate applicants to have ‘network’ compromise skills is undoubtedly due to the potential for high returns and it is claimed that the ‘average buyback’, presumably ransom paid by the victims, is between US$250,000 and US$10,000,000.

This advancement in operations is further evidenced by the December 7, 2019 announcement (Figure 6) that REvil had ‘opened a separate division’ ‘engaged in large operations’ along with revealing the compromise of CyrusOne, a Texas US-based Data Center company, and CDH Investments, a Chinese investment fund management firm.



Мы открыли отдельное подразделение, которое занимается крупными операциями. Неделю назад был осуществлен доступ к **CyrusOne.** Судя по СМИ - платить они не собираются. Очень жаль. Тактика "потратим 100 миллионов на восстановление с нуля, чем 15 на выкуп" такая же эффективная, как и оправдания Гарика Куколда Харламова. Инвесторам потом будете объяснять, где выгода. Каждая атака сопровождается копированием коммерческой информации. В случае отказа выплаты - данные будут либо проданы конкурентам, либо выкладываться в открытые источники. **GDPR**. Не хотите платить нам - платите в x10 раз больше правительству. Нет проблем.

Очень странно, что **cdhfund.com** до сих пор молчат. Они также были подвержены атаке, все данные скопированы и зашифрованы. В случае отказа - наши действия обозначены выше.

Если не отвечаем - значит не интересны. Либо мест нет.

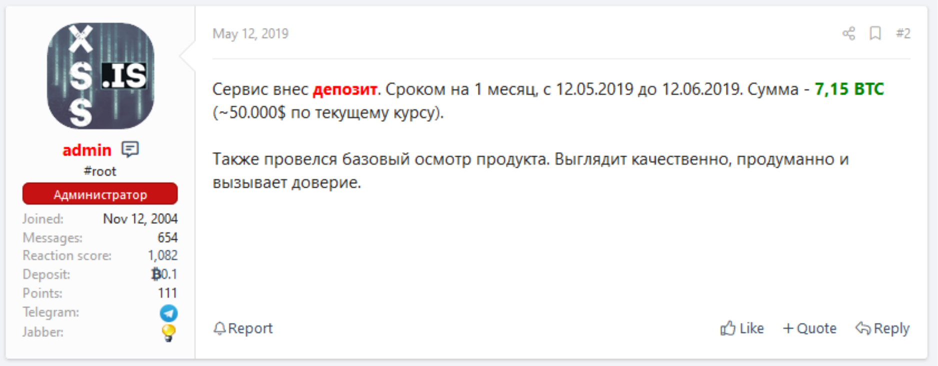
Мы открыли отдельное подразделение, которое занимается крупными операциями. Неделю назад был осуществлен доступ к **CyrusOne.** Судя по СМИ - платить они не собираются. Очень жаль. Тактика "потратим 100 миллионов на восстановление с нуля, чем 15 на выкуп" такая же эффективная, как и оправдания Гарика Куколда Харламова. Инвесторам потом будете объяснять, где выгода. Каждая атака сопровождается копированием коммерческой информации. В случае отказа выплаты - данные будут либо проданы конкурентам, либо выкладываться в открытые источники. **GDPR**. Не хотите платить нам - платите в x10 раз больше правительству. Нет проблем.

Очень странно, что **cdhfund.com** до сих пор молчат. Они также были подвержены атаке, все данные скопированы и зашифрованы. В случае отказа - наши действия обозначены выше.

Figure 6 - ‘Large operations division’ announcements

REvil Forum Reputation

In addition, REvil recently has been posting details of their 'large operations', acting as proof of their capabilities. Feedback has also been shared by others including an 'admin' of the 'XSS' cybercriminal forum. This endorsement was made when the group established themselves in May 2019 and, as well as confirming a 7.15BTC payment to the forum, worth around US$50,000 at the time, the 'admin' states that following a 'basic inspection of their product', it appears to be 'high quality, thoughtful and inspires confidence' (Figure 7).



admin
#root
Администратор

Joined: Nov 12, 2004
Messages: 654
Reaction score: 1,082
Deposit: ฿0.1
Points: 111
Telegram:
Jabber:

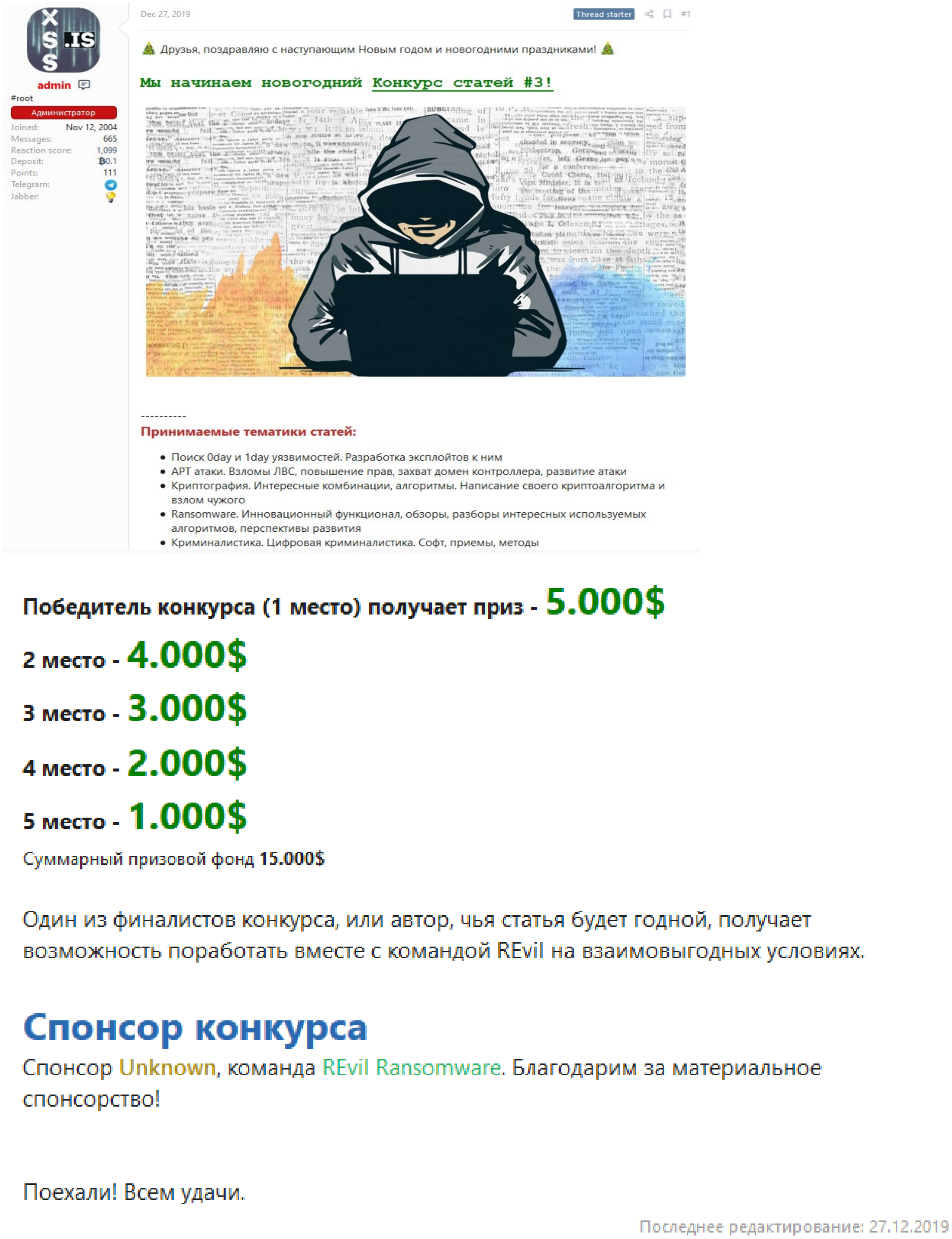
May 12, 2019 #2

Сервис внес **депозит**. Сроком на 1 месяц, с 12.05.2019 до 12.06.2019. Сумма - **7,15 BTC** (~50.000$ по текущему курсу).

Также провелся базовый осмотр продукта. Выглядит качественно, продуманно и вызывает доверие.

Figure 7 - Endorsement of REvil's 'product'

Further cementing their position within this cybercrime forum, the persona 'Unknown' of the 'REvil Ransomware Team' sponsored a 'New Year Article Contest' (Figure 8) that encourages forum participants to submit new articles to XSS forum for the chance to win up to US$5,000 in prize money, from a US$15,000 prize pot, and even the potential opportunity to work with the REvil team on 'mutually beneficial terms' for a suitably qualified finalist.



Joined: Nov 12, 2004
Messages: 665
Reaction score: 1,099
Deposit: ₿0.1
Points: 111
Telegram:
Jabber:

Dec 27, 2019

🎄 Друзья, поздравляю с наступающим Новым годом и новогодними праздниками! 🎄

Мы начинаем новогодний Конкурс статей #3!

Принимаемые тематики статей:

- Поиск 0day и 1day уязвимостей. Разработка эксплойтов к ним
- APT атаки. Взломы ЛВС, повышение прав, захват домен контроллера, развитие атаки
- Криптография. Интересные комбинации, алгоритмы. Написание своего криптоалгоритма и взлом чужого
- Ransomware. Инновационный функционал, обзоры, разборы интересных используемых алгоритмов, перспективы развития
- Криминалистика. Цифровая криминалистика. Софт, приемы, методы

Победитель конкурса (1 место) получает приз - 5.000$

2 место - 4.000$

3 место - 3.000$

4 место - 2.000$

5 место - 1.000$

Суммарный призовой фонд **15.000$**

Один из финалистов конкурса, или автор, чья статья будет годной, получает возможность поработать вместе с командой REvil на взаимовыгодных условиях.

Спонсор конкурса

Спонсор Unknown, команда REvil Ransomware. Благодарим за материальное спонсорство!

Поехали! Всем удачи.

Последнее редактирование: 27.12.2019

Figure 8 - XSS 'New Year's Article Contest #3' sponsored by Unknown/REvil Ransomware Team

In keeping with the cybercrime theme of the forum, articles are accepted on the following five topics, including:

- *Finding 0-day/1-day vulnerabilities and developing exploits*
- *APT Attacks: Hacking LANs, increasing privileges, capturing domain controllers and developing attacks*
- *Cryptography: Interesting combinations and algorithms, writing your own and hacking someone else's*
- *Ransomware: Innovative functionality, reviews, analysis and development prospects*
- *Digital forensics: Software, techniques and methods*

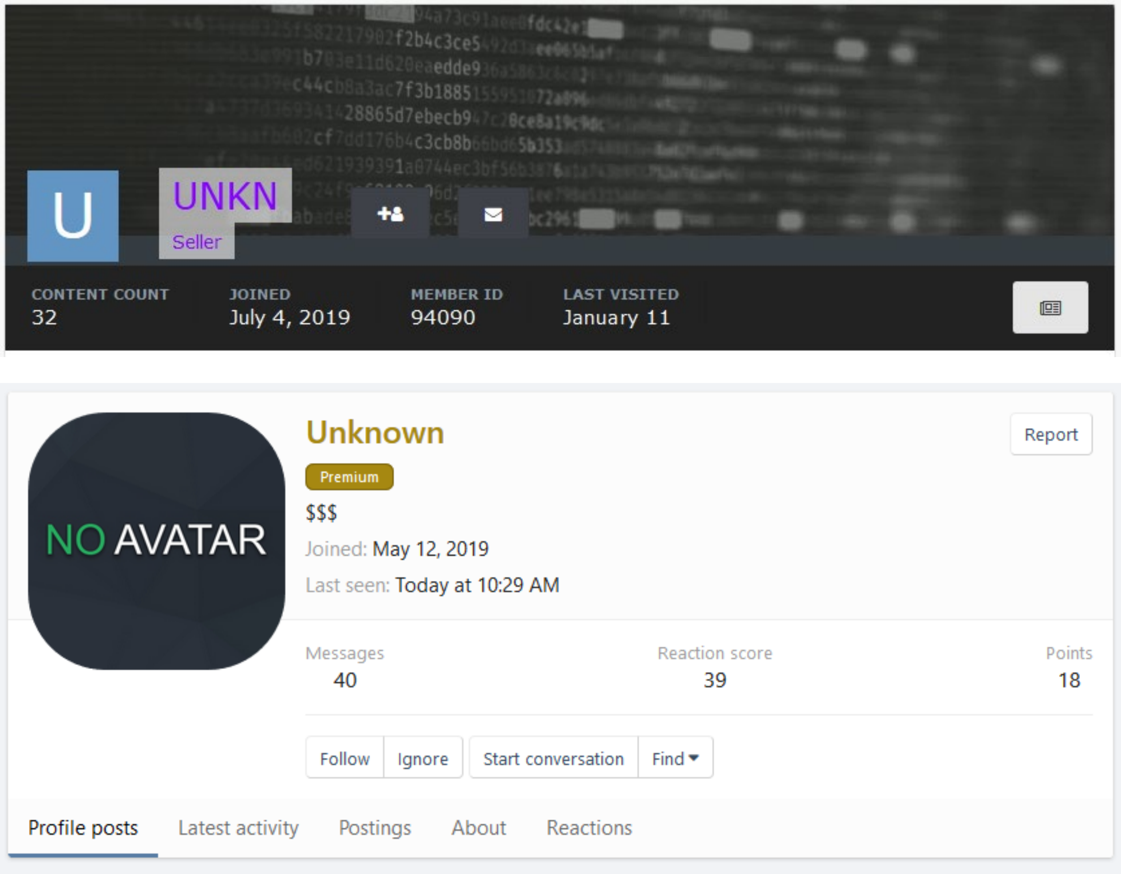
Given the sponsorship, 'Unknown' of 'REvil Ransomware Team' has weighed in on many of the submissions, sometimes offering advice and other times berating entries. With the contest running from December 28, 2019 until March 1, 2020, extended by one month from the original close date, the winners will be determined on, or after, March 2, 2020 and may well feature in future REvil campaigns, be that through the adoption of techniques detailed in their article or as a new affiliate of the group.

Threat Actor

Whilst little is known about the true identities of those behind the personas 'UNKN' and 'unknown', likely one in the same person, or the members of the 'REvil Ransomware Team', insights into their activity can be obtained by monitoring their posts on cybercriminal forums.

Based on these forum posts, it is somewhat obvious that the threat actors are Russian-speaking and are likely based in, or from, the Commonwealth of Independent States (CIS). Furthermore, they are undoubtedly experienced in the execution of a RaaS operation, with capabilities to develop enhancements to the ransomware and manage a seemingly successful affiliate program.

Those involved appear to maintain a good level of operational security and, based on the absence of relationships and historical posts, they seemingly created and started using these new personas (Figure 9) at, or around the time of, the launch of their ransomware service in May 2019.



U

UNKN

Seller

CONTENT COUNT 32

JOINED July 4, 2019

MEMBER ID 94090

LAST VISITED January 11

NO AVATAR

Unknown

Premium

$$$

Joined: May 12, 2019

Last seen: Today at 10:29 AM

Messages 40

Reaction score 39

Points 18

Figure 9 - 'Exploit' and 'XSS' forum profiles for 'UNKN' and 'Unknown'

Whilst there have been suggested links between GandCrab and REvil, no solid relationships between the REvil Ransomware Team and personas other than ‘Unknown’ and ‘UNKN’ have been determined at this time. That said, given that those behind REvil claim to be former GandCrab affiliates, it is likely that other former associates are working for, or with, the new group.

Although technical analysis of both the GandCrab and REvil ransomware binaries suggests overlap, this somewhat appears to be debunked by comments suggesting that REvil gained access to the former ransomware’s source code. Conversely, former members of GandCrab may wish to establish themselves as ‘new players’, perhaps distancing themselves from previous behaviors and associates by refuting claims of being the same threat actor.

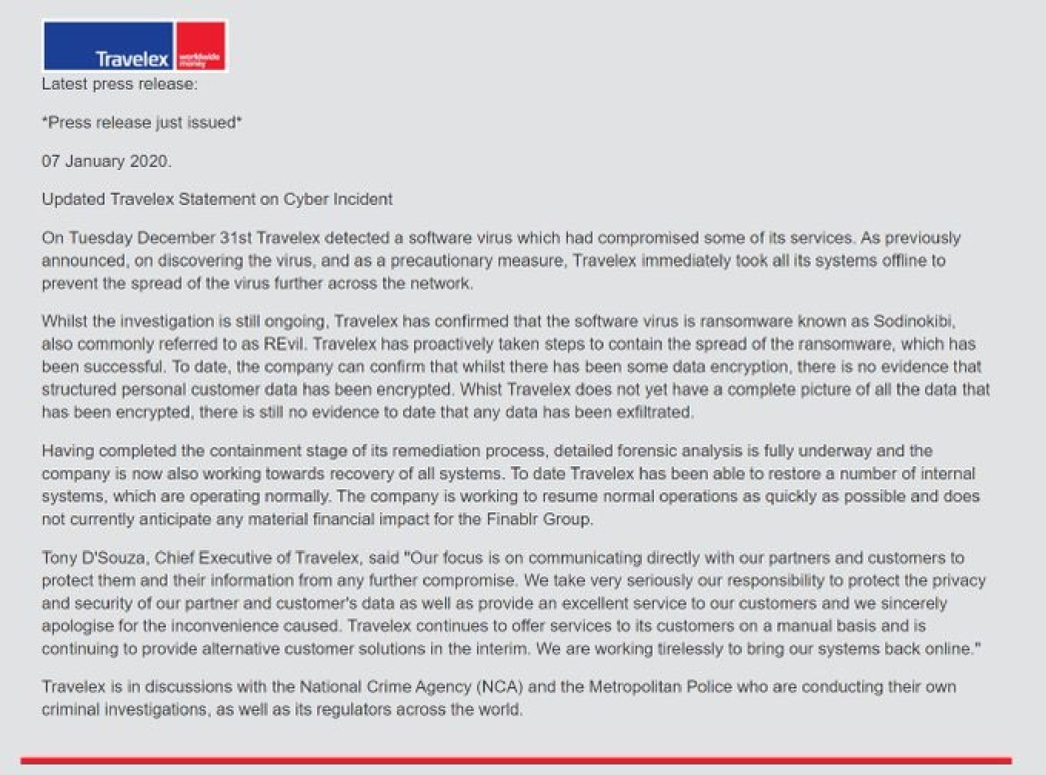
Given the affiliate program, those responsible for conducting offensive operations against networks to deploy the REvil ransomware threat could effectively originate from anywhere in the world, albeit they will likely need to be Russian-speaking to pass the interview process.

Known Victims

Travelex

Likely the most infamous of REvil's victims thus far, foreign exchange company Travelex, headquartered in the United Kingdom, detected the compromise of some of their services on 31 December 2019 resulting in their systems being taken offline including their websites, mobile applications and online exchange services.

This attack was later confirmed, in a January 7, 2020 press release (Figure 10), as being due to the REvil/Sodinokibi ransomware and culminated in the demand of a US$6 million ransom with a seven-day deadline.



Latest press release:

Press release just issued

07 January 2020.

Updated Travelex Statement on Cyber Incident

On Tuesday December 31st Travelex detected a software virus which had compromised some of its services. As previously announced, on discovering the virus, and as a precautionary measure, Travelex immediately took all its systems offline to prevent the spread of the virus further across the network.

Whilst the investigation is still ongoing, Travelex has confirmed that the software virus is ransomware known as Sodinokibi, also commonly referred to as REvil. Travelex has proactively taken steps to contain the spread of the ransomware, which has been successful. To date, the company can confirm that whilst there has been some data encryption, there is no evidence that structured personal customer data has been encrypted. Whist Travelex does not yet have a complete picture of all the data that has been encrypted, there is still no evidence to date that any data has been exfiltrated.

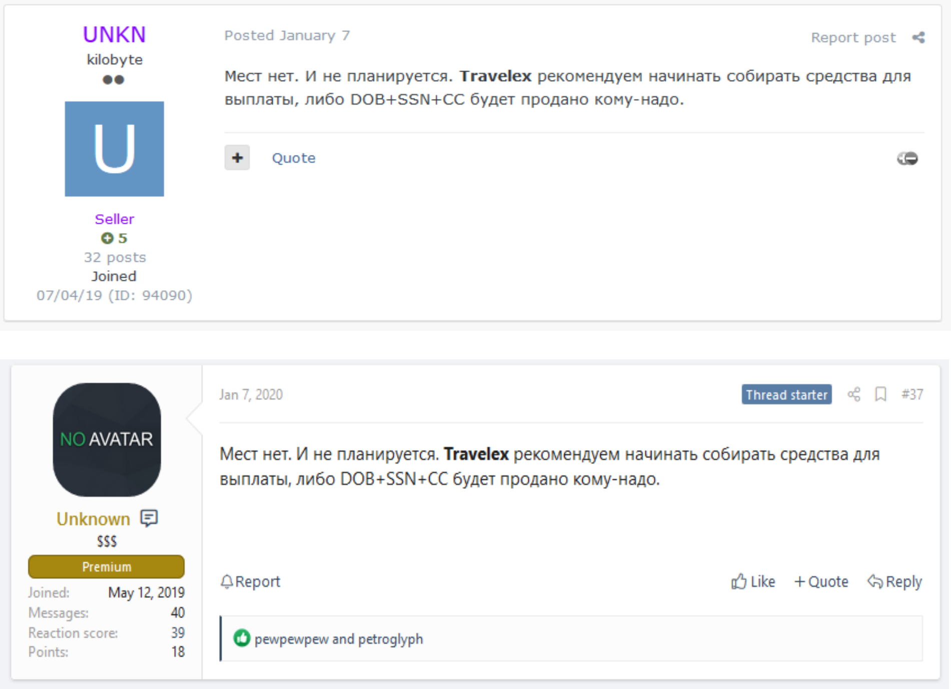
Having completed the containment stage of its remediation process, detailed forensic analysis is fully underway and the company is now also working towards recovery of all systems. To date Travelex has been able to restore a number of internal systems, which are operating normally. The company is working to resume normal operations as quickly as possible and does not currently anticipate any material financial impact for the Finablr Group.

Tony D'Souza, Chief Executive of Travelex, said "Our focus is on communicating directly with our partners and customers to protect them and their information from any further compromise. We take very seriously our responsibility to protect the privacy and security of our partner and customer's data as well as provide an excellent service to our customers and we sincerely apologise for the inconvenience caused. Travelex continues to offer services to its customers on a manual basis and is continuing to provide alternative customer solutions in the interim. We are working tirelessly to bring our systems back online."

Travelex is in discussions with the National Crime Agency (NCA) and the Metropolitan Police who are conducting their own criminal investigations, as well as its regulators across the world.

Figure 10 - Travelex Press Release (7 January 2020)

Likely in response to the January 7, 2020 press release, REvil posted on both the Exploit and XSS forums to recommend that Travelex 'raise funds for payment' as, in addition to the encrypted data, some 5GB of customer personal identifiable information (PII) was reportedly stolen (including dates of birth, social security numbers and payment card details) and would be resold if payment was not made (Figure 11).



UNKN
kilobyte
Seller
5
32 posts
Joined
07/04/19 (ID: 94090)

Posted January 7

Report post

Мест нет. И не планируется. **Travelex** рекомендуем начинать собирать средства для выплаты, либо DOB+SSN+CC будет продано кому-надо.

Unknown
$$$
Premium
Joined: May 12, 2019
Messages: 40
Reaction score: 39
Points: 18

Jan 7, 2020

Thread starter #37

Мест нет. И не планируется. **Travelex** рекомендуем начинать собирать средства для выплаты, либо DOB+SSN+CC будет продано кому-надо.

pewpewpew and petroglyph

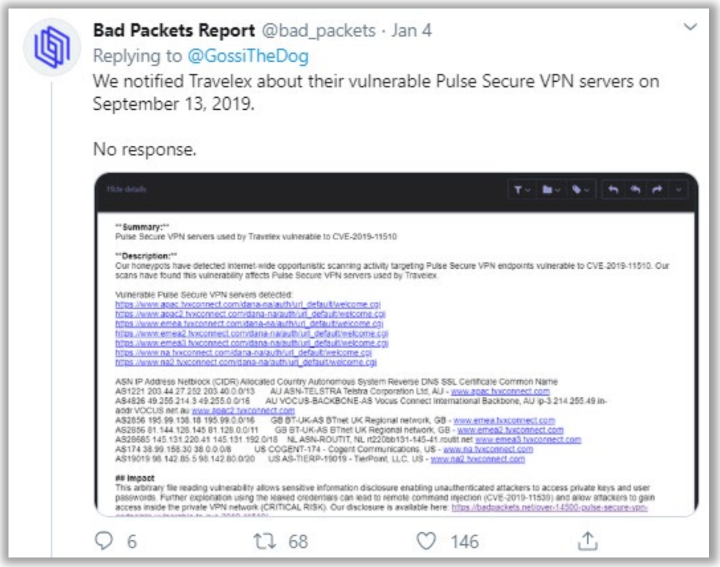
Figure 11 - Threats to resell Travelex customer data

Whilst there is no evidence of a ransom payment being made, or the stolen data being resold or leaked, Travelex suffered a long period of downtime whilst they worked throughout January and into February 2020 to restore access to many of their systems, seemingly focusing on in-store services and ATMs. As of February 5, 2020, Travelex' website and online currency exchange services, including 'white label' services for other banks, appear to remain offline.

Based on third-party observations after the compromise, it is suggested that Travelex had unpatched 'Pulse Secure VPN' nodes that could have provided a potential attack vector, especially given that attempts to notify them of being vulnerable to CVE-2019-11510[6] and CVE-2019-11539[7] appear to have been ignored (Figure 12).

[6] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510

[7] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11539



Bad Packets Report @bad_packets · Jan 4

Replying to @GossiTheDog

We notified Travelex about their vulnerable Pulse Secure VPN servers on September 13, 2019.

No response.

****Summary:****
Pulse Secure VPN servers used by Travelex vulnerable to CVE-2019-11510

****Description:****
Our honeypots have detected internet-wide opportunistic scanning activity targeting Pulse Secure VPN endpoints vulnerable to CVE-2019-11510. Our scans have found this vulnerability affects Pulse Secure VPN servers used by Travelex

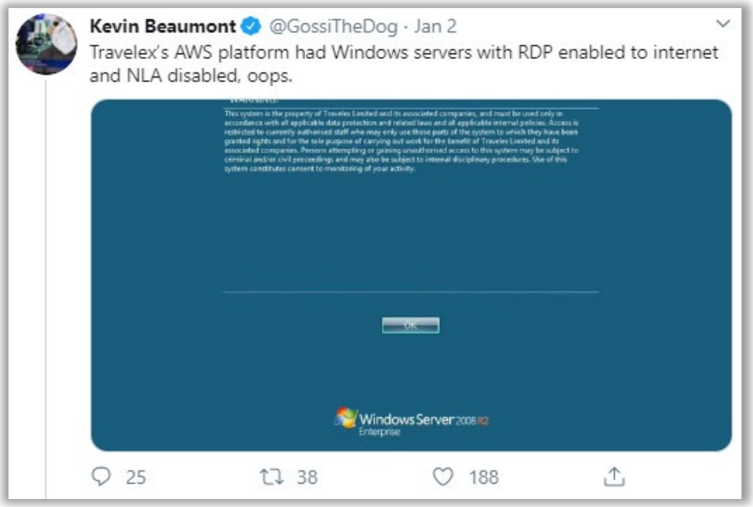
Vulnerable Pulse Secure VPN servers detected:
https://www.apac.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.apac2.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.emea.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.emea2.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.emea3.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.na.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.na2.tvxconnect.com/dana-na/auth/url_default/welcome.cgi

```
ASN IP Address Netblock (CIDR) Allocated Country Autonomous System Reverse DNS SSL Certificate Common Name
AS1221 203.44.27.252 203.40.0.0/13      AU ASN-TELSTRA Telstra Corporation Ltd, AU - www.apac.tvxconnect.com
AS4826 49.255.214.3 49.255.0.0/16      AU VOCUS-BACKBONE-AS Vocus Connect International Backbone, AU ip-3.214.255.49.in-
addr.VOCUS.net.au www.apac2.tvxconnect.com
AS2856 195.99.138.18 195.99.0.0/16      GB BT-UK-AS BTnet UK Regional network, GB - www.emea.tvxconnect.com
AS2856 81.144.128.145 81.128.0.0/11      GB BT-UK-AS BTnet UK Regional network, GB - www.emea2.tvxconnect.com
AS28685 145.131.220.41 145.131.192.0/18    NL ASN-ROUTIT, NL rt220bb131-145-41.routit.net www.emea3.tvxconnect.com
AS174 38.99.158.30 38.0.0.0/8         US COGENT-174 - Cogent Communications, US - www.na.tvxconnect.com
AS19019 98.142.85.5 98.142.80.0/20     US AS-TIERP-19019 - TierPoint, LLC, US - www.na2.tvxconnect.com
```

## Impact
This arbitrary file reading vulnerability allows sensitive information disclosure enabling unauthenticated attackers to access private keys and user passwords. Further exploitation using the leaked credentials can lead to remote command injection (CVE-2019-11539) and allow attackers to gain access inside the private VPN network (CRITICAL RISK). Our disclosure is available here: https://badpackets.net/over-14500-pulse-secure-vpn-

Figure 12 - 'Bad Packets Report' Pulse Secure VPN notification

Furthermore, and given that REvil explicitly sought affiliates with Remote Desktop Protocol (RDP) compromise skills, Travelex were identified (Figure 13) as having Windows Servers, hosted on Amazon Web Services (AWS), with RDP enabled and Network Layer Authentication (NLA) disabled.



Kevin Beaumont @GossiTheDog · Jan 2

Travelex's AWS platform had Windows servers with RDP enabled to internet and NLA disabled, oops.

WARNING:

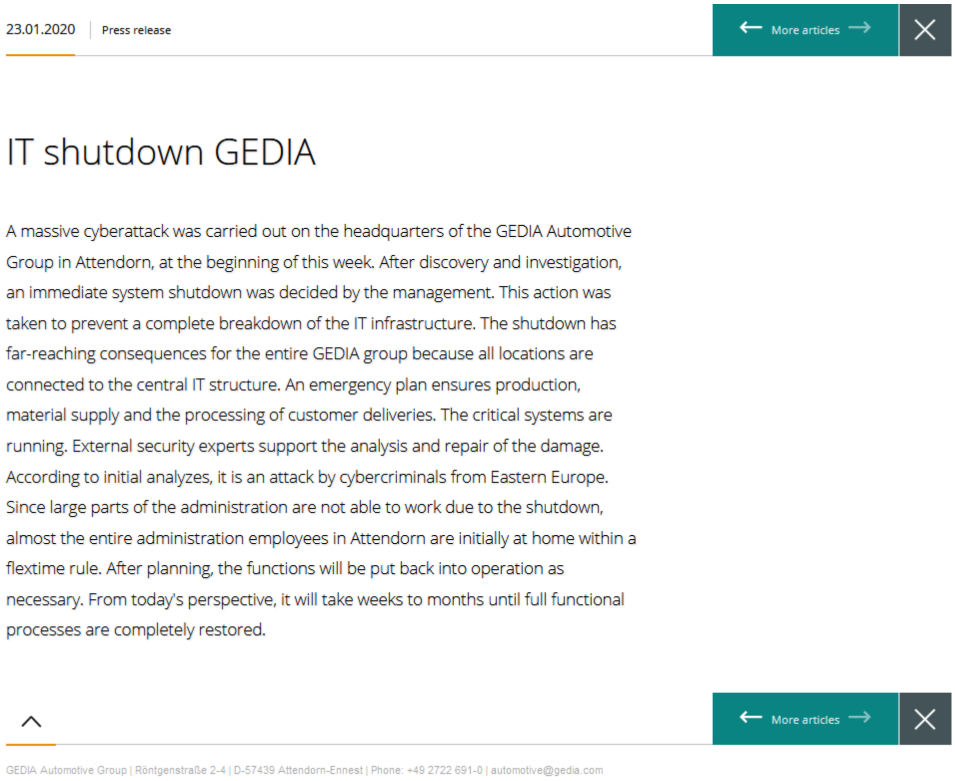
This system is the property of Travelex Limited and its associated companies, and must be used only in accordance with all applicable data protection and related laws and all applicable internal policies. Access is restricted to currently authorised staff who may only use those parts of the system to which they have been granted rights and for the sole purpose of carrying out work for the benefit of Travelex Limited and its associated companies. Persons attempting or gaining unauthorised access to this system may be subject to criminal and/or civil proceedings and may also be subject to internal disciplinary procedures. Use of this system constitutes consent to monitoring of your activity.

Figure 13 - Exposed Travelex Windows Server with RDP enabled/NLA disabled

Notably, NLA requires a client to authenticate prior to establishing a session and can help mitigate some RDP vulnerabilities.

Gedia Automotive Group

German automotive supplier Gedia Automotive Group, headquartered in Germany, discovered a 'massive cyberattack' on, or around, January 20, 2020 that, according to a since deleted press release[8] (Figure 14), resulted in 'an immediate system shutdown' and had 'far-reaching consequences' for their other business locations as these connect to their central infrastructure.



23.01.2020 | Press release

IT shutdown GEDIA

A massive cyberattack was carried out on the headquarters of the GEDIA Automotive Group in Attendorn, at the beginning of this week. After discovery and investigation, an immediate system shutdown was decided by the management. This action was taken to prevent a complete breakdown of the IT infrastructure. The shutdown has far-reaching consequences for the entire GEDIA group because all locations are connected to the central IT structure. An emergency plan ensures production, material supply and the processing of customer deliveries. The critical systems are running. External security experts support the analysis and repair of the damage. According to initial analyzes, it is an attack by cybercriminals from Eastern Europe. Since large parts of the administration are not able to work due to the shutdown, almost the entire administration employees in Attendorn are initially at home within a flextime rule. After planning, the functions will be put back into operation as necessary. From today's perspective, it will take weeks to months until full functional processes are completely restored.

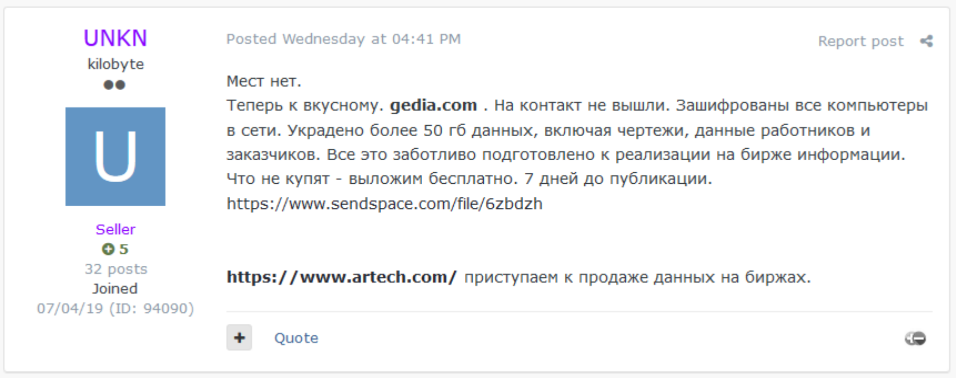
GEDIA Automotive Group | Röntgenstraße 2-4 | D-57439 Attendorn-Ennest | Phone: +49 2722 691-0 | automotive@gedia.com

Figure 14 - Gedia Press Release on January 23, 2020 (Since removed)

Consistent with REvil's TTP, posts were made to both the Exploit and XSS forums (Figure 15) indicating that 50GB of data, including blueprints, employee data and customer details, had been stolen from Gedia and would be released 'for free' if the ransom is not paid. As proof of this threat, a spreadsheet containing details of Gedia's Active Directory (AD) environment was shared and included details of AD users, policies and machines amongst other data gathered by the opensource 'ADRecon' tool[9].

[8] https://www.gedia.com/en/news/article/IT

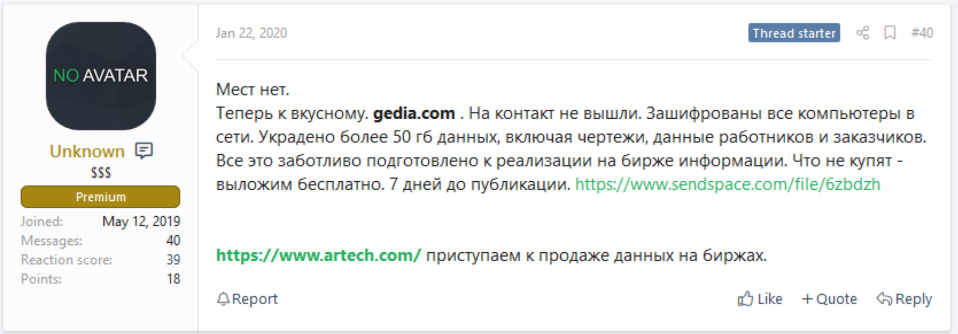
[9] https://github.com/sense-of-security/ADRecon



Posted Wednesday at 04:41 PM

Мест нет.
Теперь к вкусному. **gedia.com** . На контакт не вышли. Зашифрованы все компьютеры в сети. Украдено более 50 гб данных, включая чертежи, данные работников и заказчиков. Все это заботливо подготовлено к реализации на бирже информации. Что не купят - выложим бесплатно. 7 дней до публикации.
https://www.sendspace.com/file/6zbdzh

https://www.artech.com/ приступаем к продаже данных на биржах.



Joined:	May 12, 2019
Messages:	40
Reaction score:	39
Points:	18

Jan 22, 2020

Мест нет.
Теперь к вкусному. **gedia.com** . На контакт не вышли. Зашифрованы все компьютеры в сети. Украдено более 50 гб данных, включая чертежи, данные работников и заказчиков. Все это заботливо подготовлено к реализации на бирже информации. Что не купят - выложим бесплатно. 7 дней до публикации. https://www.sendspace.com/file/6zbdzh

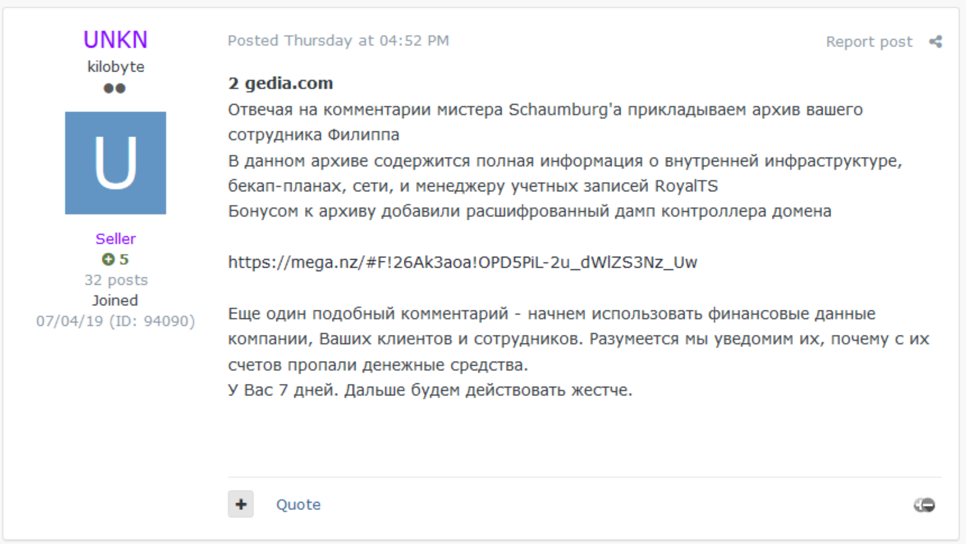
https://www.artech.com/ приступаем к продаже данных на биржах.

Figure 15 - Gedia 'ADRecon' file leak

Note: *These posts also reference an additional victim - US-based 'Artech Information Systems'.*

ADRecon is a post-compromise tool, and the data shared by Gedia may be beneficial to other attackers given the level of detail available within the spreadsheet.

Following the distribution of Gedia's press release on January 23, 2020 and 'comments', reportedly denying any data theft, made by Gedia's CEO Markus Schaumburg, a 1.55GB archive of data seemingly stolen from an IT department employee was shared in both 'Exploit' and 'XSS' forum posts (Figure 16).



UNKN
kilobyte
Seller
5
32 posts
Joined
07/04/19 (ID: 94090)

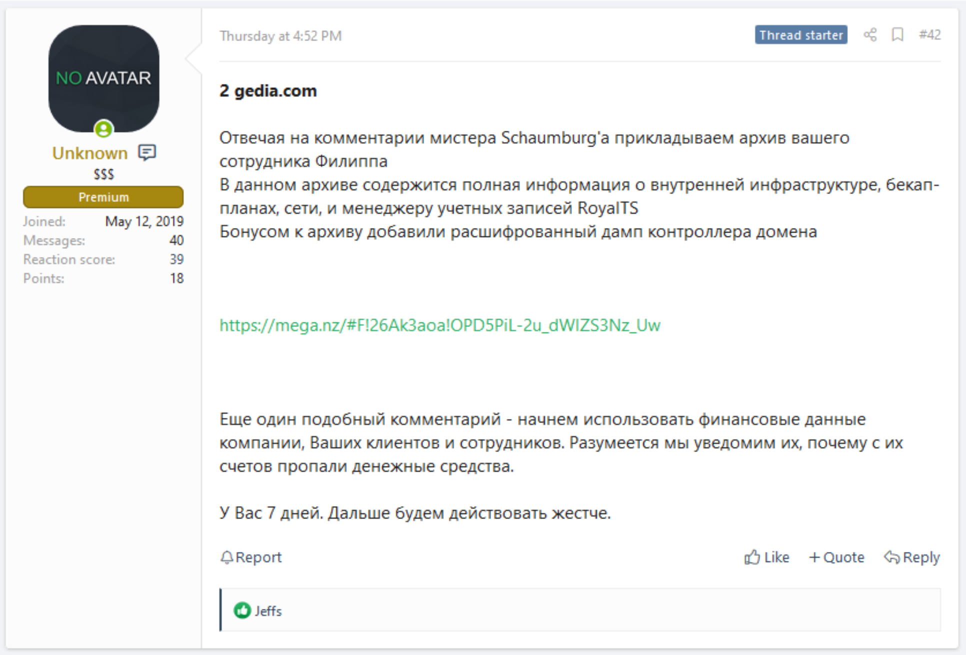
Posted Thursday at 04:52 PM

Report post

2 gedia.com
Отвечая на комментарии мистера Schaumburg'а прикладываем архив вашего сотрудника Филиппа
В данном архиве содержится полная информация о внутренней инфраструктуре, бекап-планах, сети, и менеджеру учетных записей RoyalTS
Бонусом к архиву добавили расшифрованный дамп контроллера домена

https://mega.nz/#F!26Ak3aoa!OPD5PiL-2u_dWlZS3Nz_Uw

Еще один подобный комментарий - начнем использовать финансовые данные компании, Ваших клиентов и сотрудников. Разумеется мы уведомим их, почему с их счетов пропали денежные средства.
У Вас 7 дней. Дальше будем действовать жестче.



Unknown
$$$
Premium
Joined: May 12, 2019
Messages: 40
Reaction score: 39
Points: 18

Thursday at 4:52 PM

2 gedia.com

Отвечая на комментарии мистера Schaumburg'а прикладываем архив вашего сотрудника Филиппа
В данном архиве содержится полная информация о внутренней инфраструктуре, бекап-планах, сети, и менеджеру учетных записей RoyalTS
Бонусом к архиву добавили расшифрованный дамп контроллера домена

https://mega.nz/#F!26Ak3aoa!OPD5PiL-2u_dWlZS3Nz_Uw

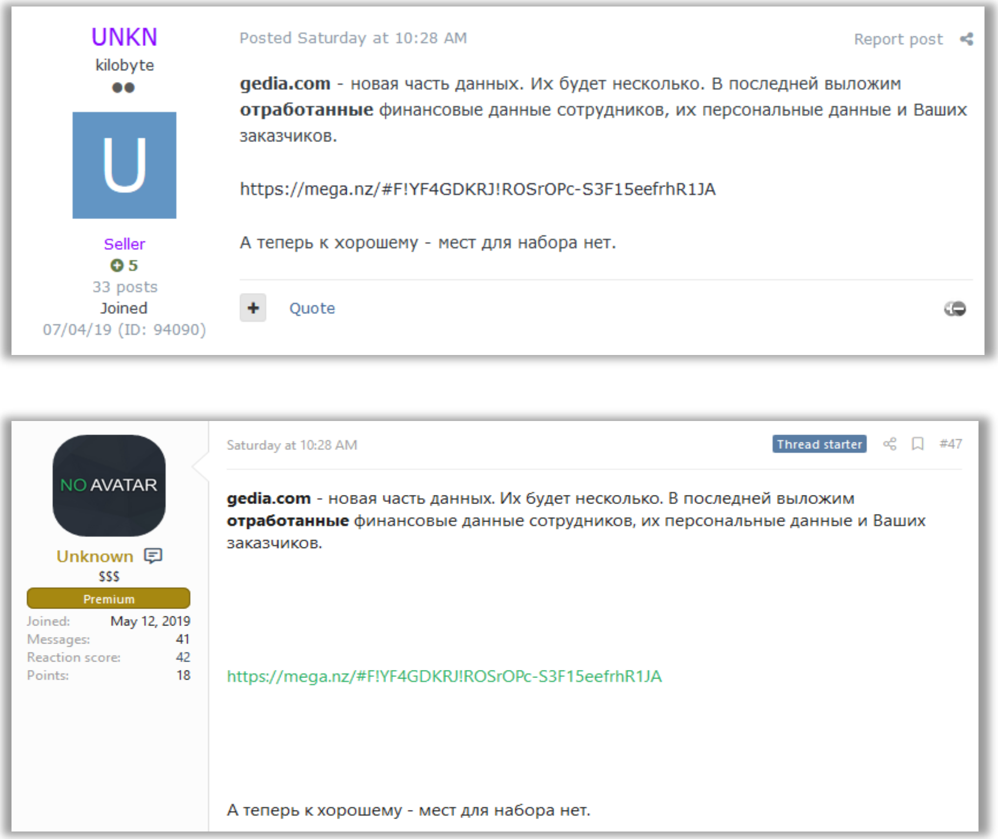
Еще один подобный комментарий - начнем использовать финансовые данные компании, Ваших клиентов и сотрудников. Разумеется мы уведомим их, почему с их счетов пропали денежные средства.

У Вас 7 дней. Дальше будем действовать жестче.

Figure 16 - Gedia IT data leak

Aside from documentation relating to Gedia's IT infrastructure, the archive included potential plain text keys and passwords, although much of the data, based on timestamps, appeared to be more than two years old. Regardless of its age, as with any data of this nature, it can provide valuable intelligence to other threat actors seeking to attack or compromise the organization further.

Further proving the seriousness of these attacks and REvil's intent to act on their threats, January 27, 2020 saw the release (Figure 17) of another Gedia stolen data set named 'gedia-audi-first-part' which appears to include some 15GB of design and commercial data related to parts for Audi, Porsche and Volkswagen vehicles.



UNKN
kilobyte
Seller
5
33 posts
Joined
07/04/19 (ID: 94090)

Posted Saturday at 10:28 AM

gedia.com - новая часть данных. Их будет несколько. В последней выложим **отработанные** финансовые данные сотрудников, их персональные данные и Ваших заказчиков.

https://mega.nz/#F!YF4GDKRJ!ROSrOPc-S3F15eefrhR1JA

А теперь к хорошему - мест для набора нет.

Unknown
$$$
Premium
Joined: May 12, 2019
Messages: 41
Reaction score: 42
Points: 18

Saturday at 10:28 AM

gedia.com - новая часть данных. Их будет несколько. В последней выложим **отработанные** финансовые данные сотрудников, их персональные данные и Ваших заказчиков.

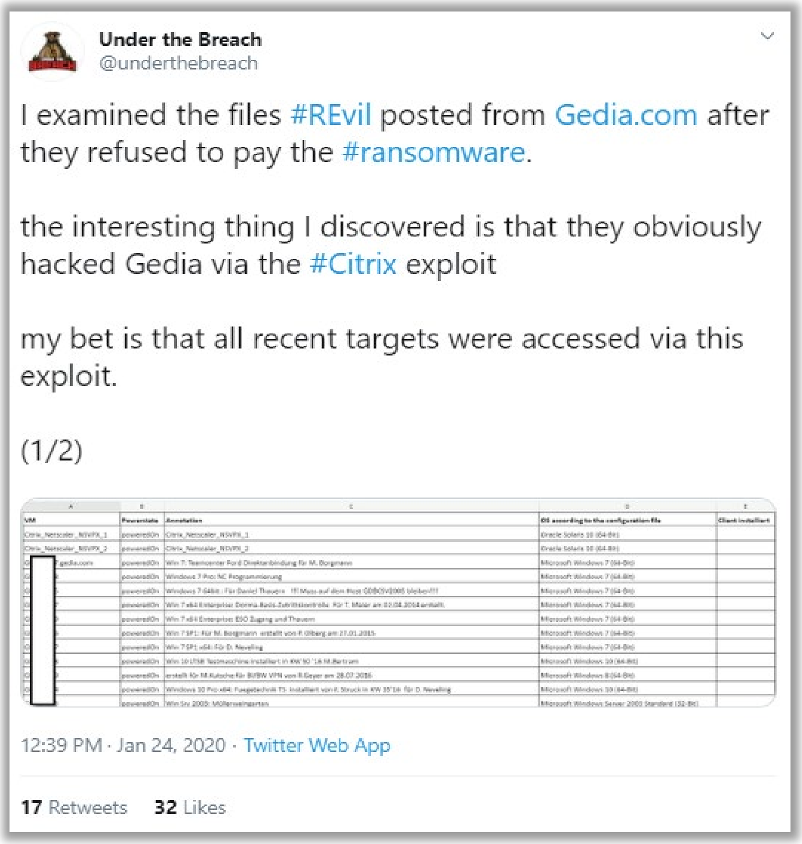
https://mega.nz/#F!YF4GDKRJ!ROSrOPc-S3F15eefrhR1JA

А теперь к хорошему - мест для набора нет.

Figure 17 - Gedia design and commercial data leak

Based on third-party analysis of Gedia's IT data leak and the identification of Citrix virtual machine documentation (Figure 18), it was suggested that these may have been vulnerable to CVE-2019-19781[10], a directory traversal and remote code execution vulnerability on some versions of Citrix Application Delivery Controllers (ADC) and Gateways. Proof-of-concept (PoC) exploit code was made available for this vulnerability on January 10, 2020, potentially aligning with the Gedia compromise and supporting this hypothesis.

[10] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19781



Under the Breach
@underthebreach

I examined the files #REvil posted from Gedia.com after they refused to pay the #ransomware.

the interesting thing I discovered is that they obviously hacked Gedia via the #Citrix exploit

my bet is that all recent targets were accessed via this exploit.

(1/2)

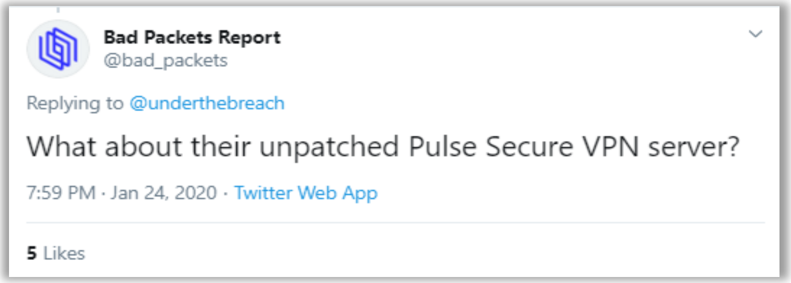
A	B	C	D	E
VM	Powerstate	Annotation	OS according to the configuration file	Client installiert
Citrix_Netscaler_NSVPX_1	poweredOn	Citrix_Netscaler_NSVPX_1	Oracle Solaris 10 (64-Bit)	
Citrix_Netscaler_NSVPX_2	poweredOn	Citrix_Netscaler_NSVPX_2	Oracle Solaris 10 (64-Bit)	
[redacted]	poweredOn	Win 7: Teamcenter Ford Direktanbindung für M. Borgmann	Microsoft Windows 7 (64-Bit)	
[redacted]	poweredOn	Windows 7 Pro: NC Programmierung	Microsoft Windows 7 (64-Bit)	
[redacted]	poweredOn	Windows 7 64bit : Für Daniel Thauern !!! Muss auf dem Host GDBCSV2005 bleiben!!!	Microsoft Windows 7 (64-Bit)	
[redacted]	poweredOn	Win 7 x64 Enterprise: Dorma Basis-Zutrittskontrolle. Für T. Maier am 02.04.2014 erstellt.	Microsoft Windows 7 (64-Bit)	
[redacted]	poweredOn	Win 7 x64 Enterprise: ESO Zugang und Thauern	Microsoft Windows 7 (64-Bit)	
[redacted]	poweredOn	Win 7 SP1: Für M. Borgmann erstellt von F. Olberg am 27.01.2015	Microsoft Windows 7 (64-Bit)	
[redacted]	poweredOn	Win 7 SP1 x64: Für D. Nevelling	Microsoft Windows 7 (64-Bit)	
[redacted]	poweredOn	Win 10 LTSB Testmaschine installiert in KW 50 '16 M.Bertram	Microsoft Windows 10 (64-Bit)	
[redacted]	poweredOn	erstellt für M.Kutsche für BVBW VPN von R.Geyer am 28.07.2016	Microsoft Windows 8 (64-Bit)	
[redacted]	poweredOn	Windows 10 Pro x64: Fuegetechnik TS installiert von F. Struck in KW 35'16 für D. Nevelling	Microsoft Windows 10 (64-Bit)	
[redacted]	poweredOn	Win Srv 2003: Müllerweingarten	Microsoft Windows Server 2003 Standard (32-Bit)	

12:39 PM · Jan 24, 2020 · Twitter Web App

17 Retweets 32 Likes

Figure 18 - Gedia Citrix CVE-2019-19781 hypothesis

Additionally, 'Bad Packets' respond (Figure 19) to this tweet and suggest that Gedia may have had an unpatched Pulse Secure VPN node that could have been exploited by REvil, as suggested in the Travelex incident.



Bad Packets Report
@bad_packets

Replying to @underthebreach

What about their unpatched Pulse Secure VPN server?

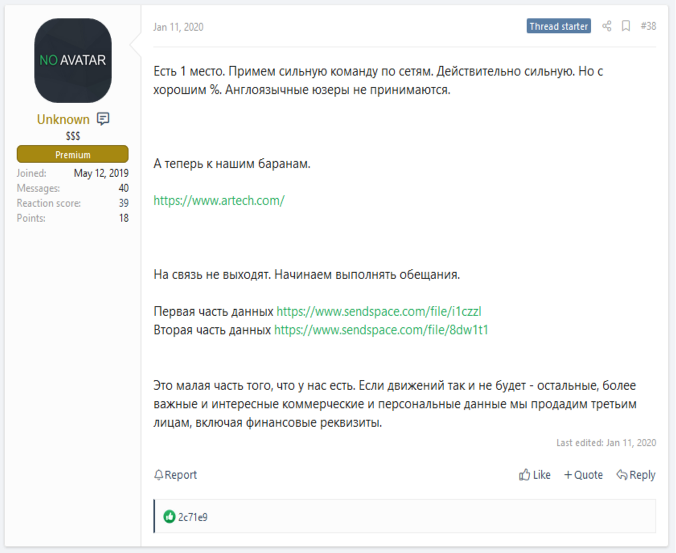
7:59 PM · Jan 24, 2020 · Twitter Web App

5 Likes

Figure 19 - Bad Packets suggest Pulse Secure VPN exploited

Artech Information Systems

Whilst US-based Artech Information Systems, an IT staffing company, hasn’t appeared publish an official statement regarding a potential compromise and/or ransomware attack, those behind REvil posted a sample set of Artech’s data on both the ‘Exploit’ and ‘XSS’ forums on January 11, 2020 (Figure 20).



Joined:	May 12, 2019
Messages:	40
Reaction score:	39
Points:	18

Jan 11, 2020 Thread starter #38

Есть 1 место. Примем сильную команду по сетям. Действительно сильную. Но с хорошим %. Англоязычные юзеры не принимаются.

А теперь к нашим баранам.

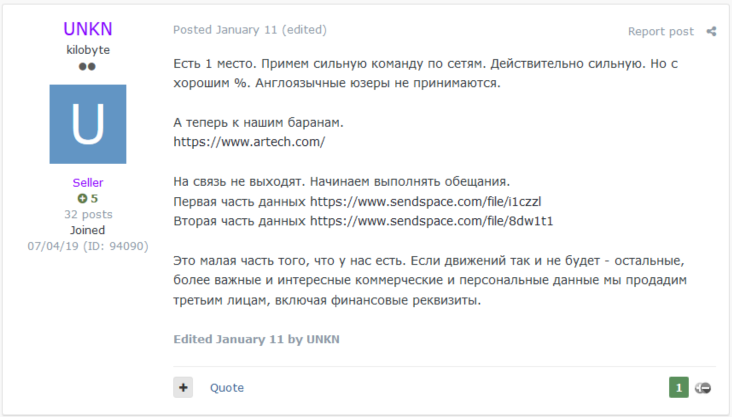
https://www.artech.com/

На связь не выходят. Начинаем выполнять обещания.

Первая часть данных https://www.sendspace.com/file/i1czzl
Вторая часть данных https://www.sendspace.com/file/8dw1t1

Это малая часть того, что у нас есть. Если движений так и не будет - остальные, более важные и интересные коммерческие и персональные данные мы продадим третьим лицам, включая финансовые реквизиты.

Last edited: Jan 11, 2020



Posted January 11 (edited) Report post

Есть 1 место. Примем сильную команду по сетям. Действительно сильную. Но с хорошим %. Англоязычные юзеры не принимаются.

А теперь к нашим баранам.
https://www.artech.com/

На связь не выходят. Начинаем выполнять обещания.
Первая часть данных https://www.sendspace.com/file/i1czzl
Вторая часть данных https://www.sendspace.com/file/8dw1t1

Это малая часть того, что у нас есть. Если движений так и не будет - остальные, более важные и интересные коммерческие и персональные данные мы продадим третьим лицам, включая финансовые реквизиты.

Edited January 11 by UNKN

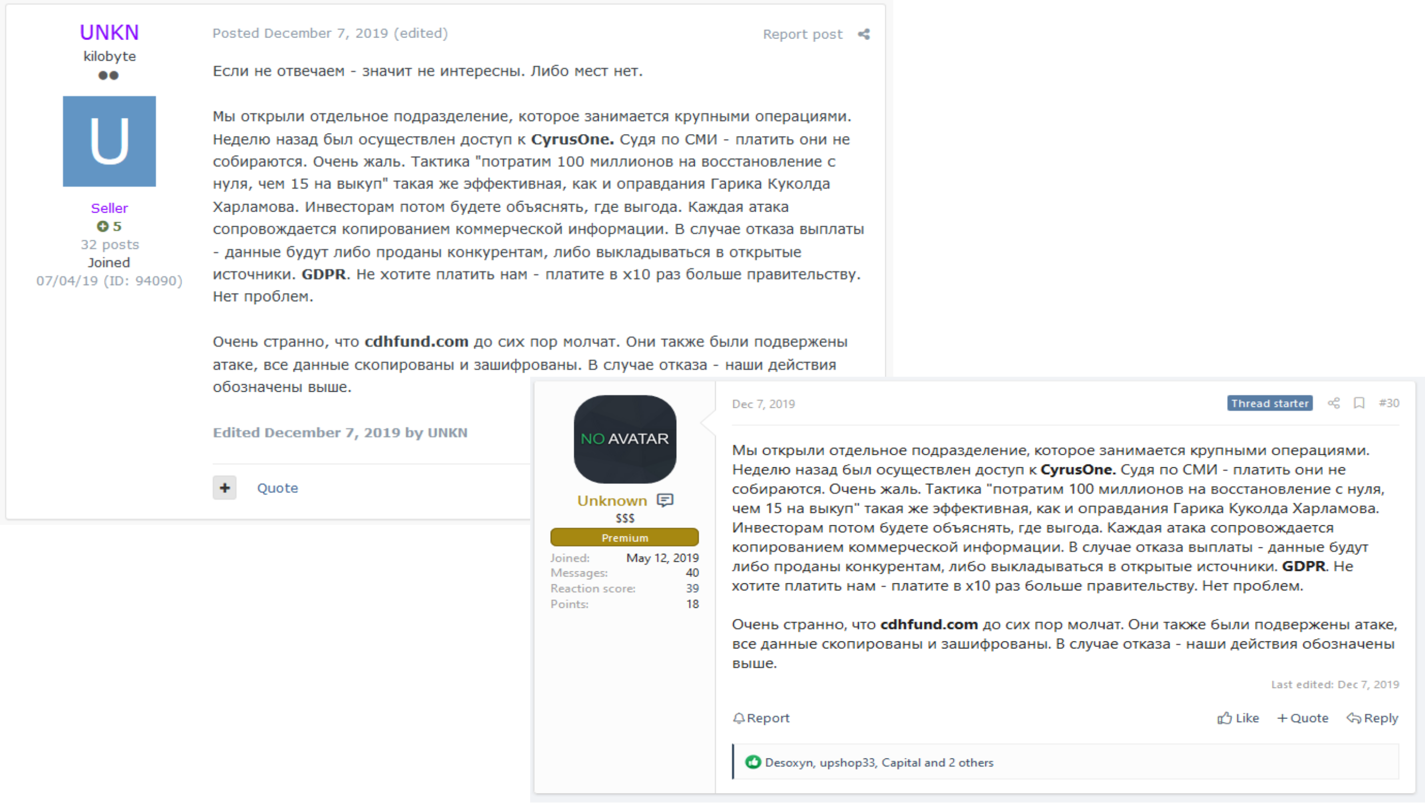
Figure 20 - Artech data leak

The data leaked in this instance included the output of the opensource ADRecon tool, predating it’s use against Gedia, along with a 300MB archive containing data seemingly belonging to an IT department. As subsequently seen in the Gedia data leaks, IT department data includes a treasure-trove of intelligence on the organization’s infrastructure as well as potential plaintext keys and passwords that can be abused in other attacks.

CyrusOne / CDH Investments

Data center and managed service provider CyrusOne, headquartered in the United States, confirmed a ransomware incident in a December 5, 2019 press release[11] as impacting their managed service division and causing 'availability issues' for six managed service customers primarily serviced by their New York data center. Additionally, CDH Investments, a Chinese investment fund firm, appears to have been compromised by REvil around a similar time although no official announcement has been made.

Whilst there was little public information surrounding the incident, forum posts on both the 'Exploit' and 'XSS' forums (Figure 21) are significant in that they signify the start of REvil's 'separate division', that is focused on large operations. As seen in more recent attacks, REvil claim to have stolen data from CyrusOne and CDH Investments although no leaks have been observed to date.



UNKN
kilobyte
Seller
5
32 posts
Joined
07/04/19 (ID: 94090)

Posted December 7, 2019 (edited)

Report post

Если не отвечаем - значит не интересны. Либо мест нет.

Мы открыли отдельное подразделение, которое занимается крупными операциями. Неделю назад был осуществлен доступ к **CyrusOne.** Судя по СМИ - платить они не собираются. Очень жаль. Тактика "потратим 100 миллионов на восстановление с нуля, чем 15 на выкуп" такая же эффективная, как и оправдания Гарика Куколда Харламова. Инвесторам потом будете объяснять, где выгода. Каждая атака сопровождается копированием коммерческой информации. В случае отказа выплаты - данные будут либо проданы конкурентам, либо выкладываться в открытые источники. **GDPR**. Не хотите платить нам - платите в x10 раз больше правительству. Нет проблем.

Очень странно, что **cdhfund.com** до сих пор молчат. Они также были подвержены атаке, все данные скопированы и зашифрованы. В случае отказа - наши действия обозначены выше.

Edited December 7, 2019 by UNKN

+ Quote

NO AVATAR
Unknown
$$$
Premium

Joined:	May 12, 2019
Messages:	40
Reaction score:	39
Points:	18

Dec 7, 2019

Thread starter #30

Мы открыли отдельное подразделение, которое занимается крупными операциями. Неделю назад был осуществлен доступ к **CyrusOne.** Судя по СМИ - платить они не собираются. Очень жаль. Тактика "потратим 100 миллионов на восстановление с нуля, чем 15 на выкуп" такая же эффективная, как и оправдания Гарика Куколда Харламова. Инвесторам потом будете объяснять, где выгода. Каждая атака сопровождается копированием коммерческой информации. В случае отказа выплаты - данные будут либо проданы конкурентам, либо выкладываться в открытые источники. **GDPR**. Не хотите платить нам - платите в x10 раз больше правительству. Нет проблем.

Очень странно, что **cdhfund.com** до сих пор молчат. Они также были подвержены атаке, все данные скопированы и зашифрованы. В случае отказа - наши действия обозначены выше.

Last edited: Dec 7, 2019

Report

Like + Quote Reply

Desoxyn, upshop33, Capital and 2 others

Figure 21 - REvil separate division announcement along with identification of CyrusOne and CDH Funds as victims

[11] https://investor.cyrusone.com/news-releases/news-release-details/managed-service-division-cyrusone-addresses-ransomware-incident

Paying Victims

Often not advocated by law enforcement agencies[12], especially as encourages further attacks, some victims may feel compelled to pay ransoms, especially where they lack the capabilities to successfully restore their systems in a reasonable timeframe.

Whilst the true scale of REvil's victims cannot be fully assessed, especially as some may pay for restoration and to protect their anonymity, two organizations have been identified as paying to recover from their REvil ransomware attacks.

The most recent, *Albany International Airport* in the United States was subject to a ransomware attack that was discovered on December 25, 2019 and was reported as only impacting their administrative data rather than any traveler data or airport operations. Subsequently, the airport authority's insurance provider authorized the payment of an "under six figures" ransom, made using the bitcoin (BTC) cryptocurrency on December 30, 2019 and decryption keys were made available two hours later allowing the restoration of data.

Earlier in 2019, *PerCSoft*, a US-based provider of cloud services to Digital Dental Records (DDR), suffered a ransomware attack on the morning of August 26, 2019 that lead to the encryption of DDR's dental records which impacted around 400 dental practices across the United States. Based on a report by investigative reporter Brian Krebs[13], screenshots obtained from a private Facebook group suggest that the ransom was paid and access to the decryption keys was gained (Figure 22).

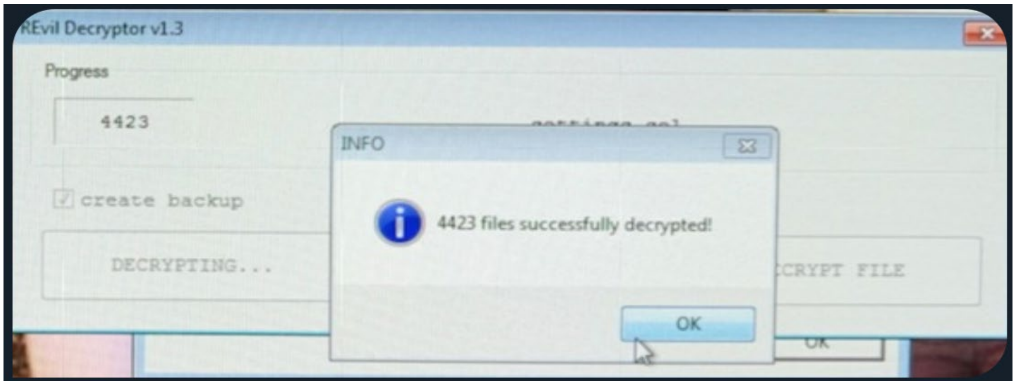
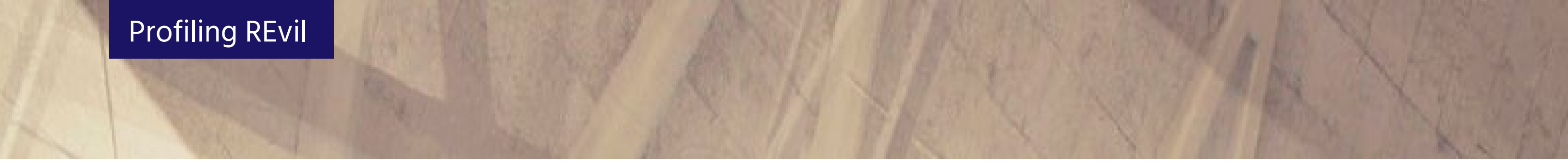

4423 files successfully decrypted!

Figure 22 - REvil Decprytor screenshot reportedly from the PerCSoft/DDR incident *(Image source: Krebs on Security)*

[12] https://www.ic3.gov/media/2019/191002.aspx

[13] https://krebsonsecurity.com/2019/08/ransomware-bites-dental-data-backup-firm/



Contact Information

ISRAEL
Tel:+972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM
Tel:+44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE
Tel:+65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA
Tel:+1-646-568-7813
214 W 29th St, 2nd Floor New York,NY 10001

LATAM
Tel:+507-395-1553
Panama City

Cyberint