

Cyber threats in 2021

The hidden evil

Dr. Amin Hasbini
Global Research and Analysis team
Head of research center, META

kaspersky BRING ON
THE FUTURE



Agenda

1. Introduction
2. What we do and how do we do it
3. The status of cybersecurity in 2022
4. Upcoming threat predictions

Expertise

>4,000

highly qualified
specialists

1/3

of our employees are
R&D specialists

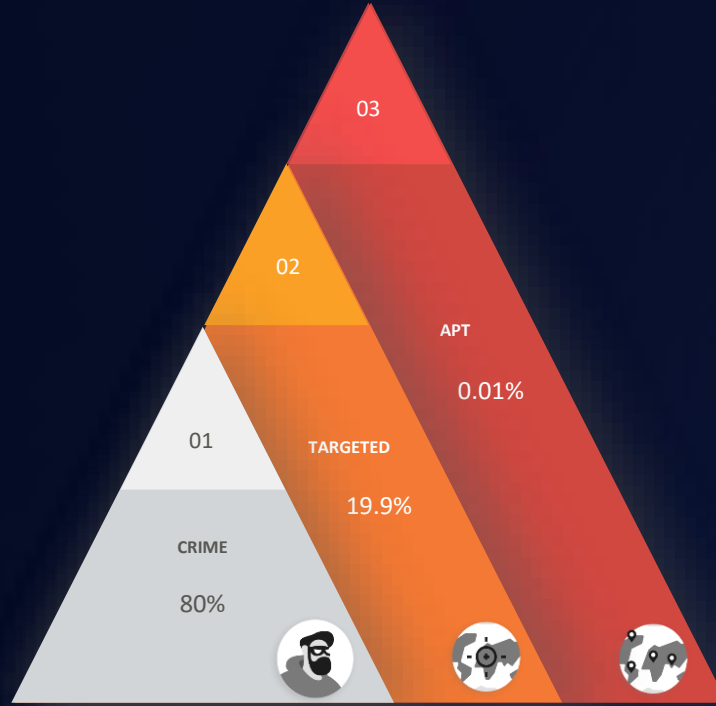
40+

world-leading
security experts:
our elite group



Our unique team of security experts are at the forefront of protecting people around the world from the most sophisticated and dangerous cyberthreats. This expertise enriches our state-of-the-art protection technologies, making their quality unsurpassed.

Kinds of threats targeting users and organizations



Advanced Persistent Threat (APT)

Case study : TURLA APT– an introduction

- Not your everyday encounter
- A Global multi-platform multi-faceted threat actor
- A regular developer/employer of advanced techniques and zero-day exploits

TURLA APT— also known as

Epic Turla
Snake/Uroboros
Mosquito Turla
Phoenix Turla
Penguin Turla
Ugly Turla
Gloog/ClickyGloog
IcedCoffee + KopiLuwak
WhiteAtlas
Neurons - Dark and Light
Agent.btz+dne
PNGDropper
WhiteBear
TurlaSat

VENOMOUS Bear
Group 88
APT 29
Belugasturgeon
Waterbug
WRAITH
Pfinet
TAG_0530
KRYPTON
Hippo Team
Pacifier APT
Popeye
SIG23
Iron Hunter
MAKERSMARK
...

1-TURLA APT— early traces

Pentagon computer networks attacked

BY JULIAN E. BARNES
NOV. 28, 2008 12 AM PT

BARNES IS A WRITER IN OUR WASHINGTON BUREAU.
WASHINGTON —

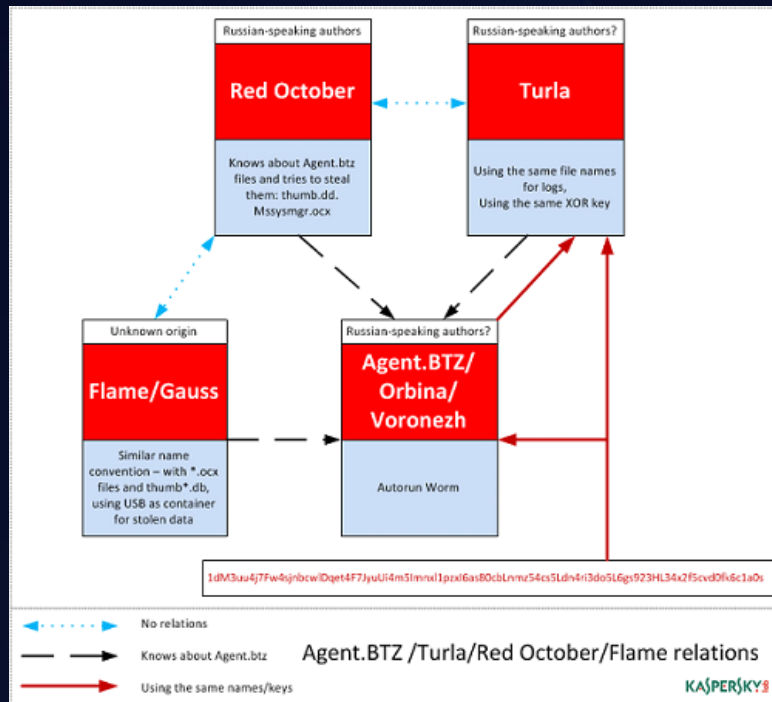
Senior military leaders took the exceptional step of briefing President Bush this week on a severe and widespread electronic attack on Defense Department

Officials would not describe the exact threat from agent.btz, or say whether it could shut down computers or steal information. Some computer experts have reported that agent.btz can allow an attacker to take control of a computer remotely and to take files and other information from it.

Agent.btz: a Source of Inspiration?

APT REPORTS

12 MAR 2014



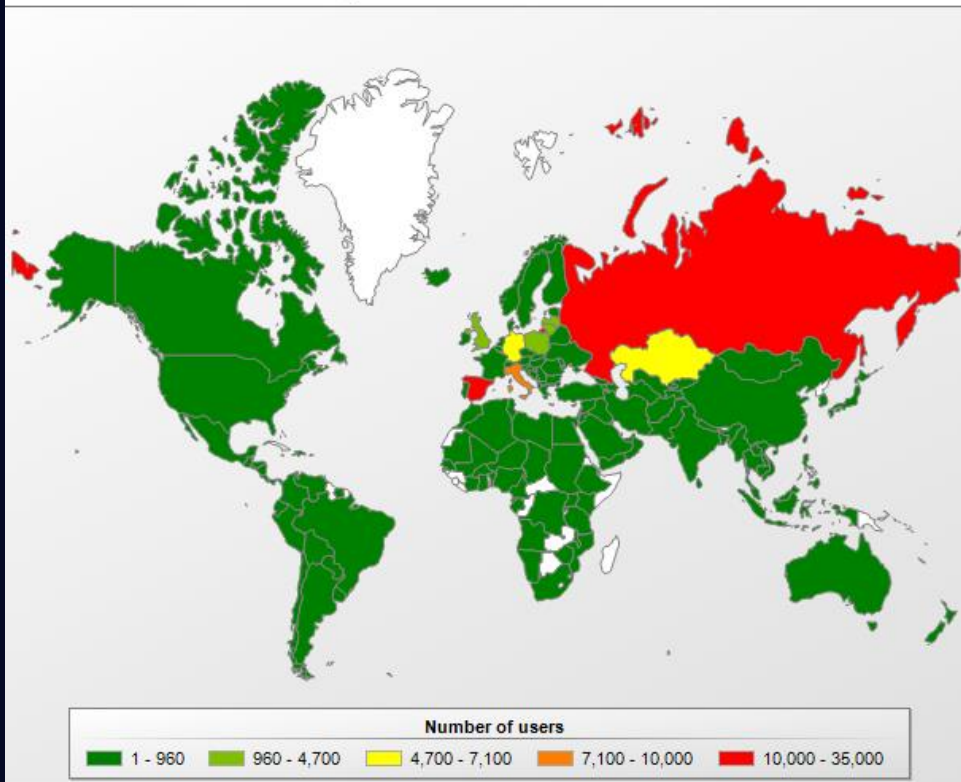
1-TURLA APT— early traces

Agent.btz: a Source of Inspiration?

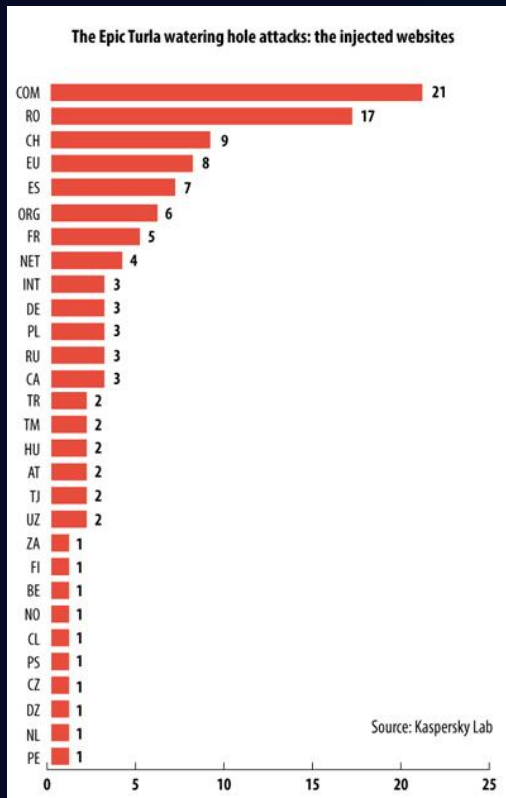
APT REPORTS

12 MAR 2014

Agent.btz distribution 2011-2013



2-TURLA APT– Epic Turla (~2013-2015)



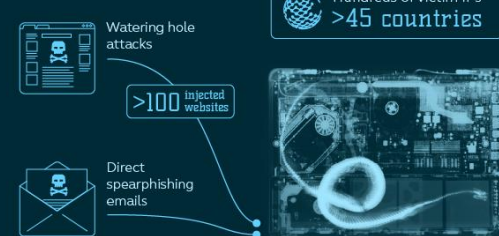
The Epic Snake: Unraveling the mysteries of the Turla cyber-espionage campaign



Epic Turla: The early-stage infection mechanism

Mission: Attackers inject the Epic backdoor into the high-profile victim's PC to validate the identity thereof

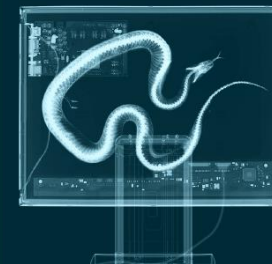
Infection vectors:



Targets:



Cobra system and Snake malware platform



Cobra Carbon system/ Pfinet (+others):

Intermediary upgrades and communication plugins.

Snake/Uroburos:

High-grade malware platform that includes a rootkit and virtual file systems

2-TURLA APT– Epic Turla (~2013-2015)

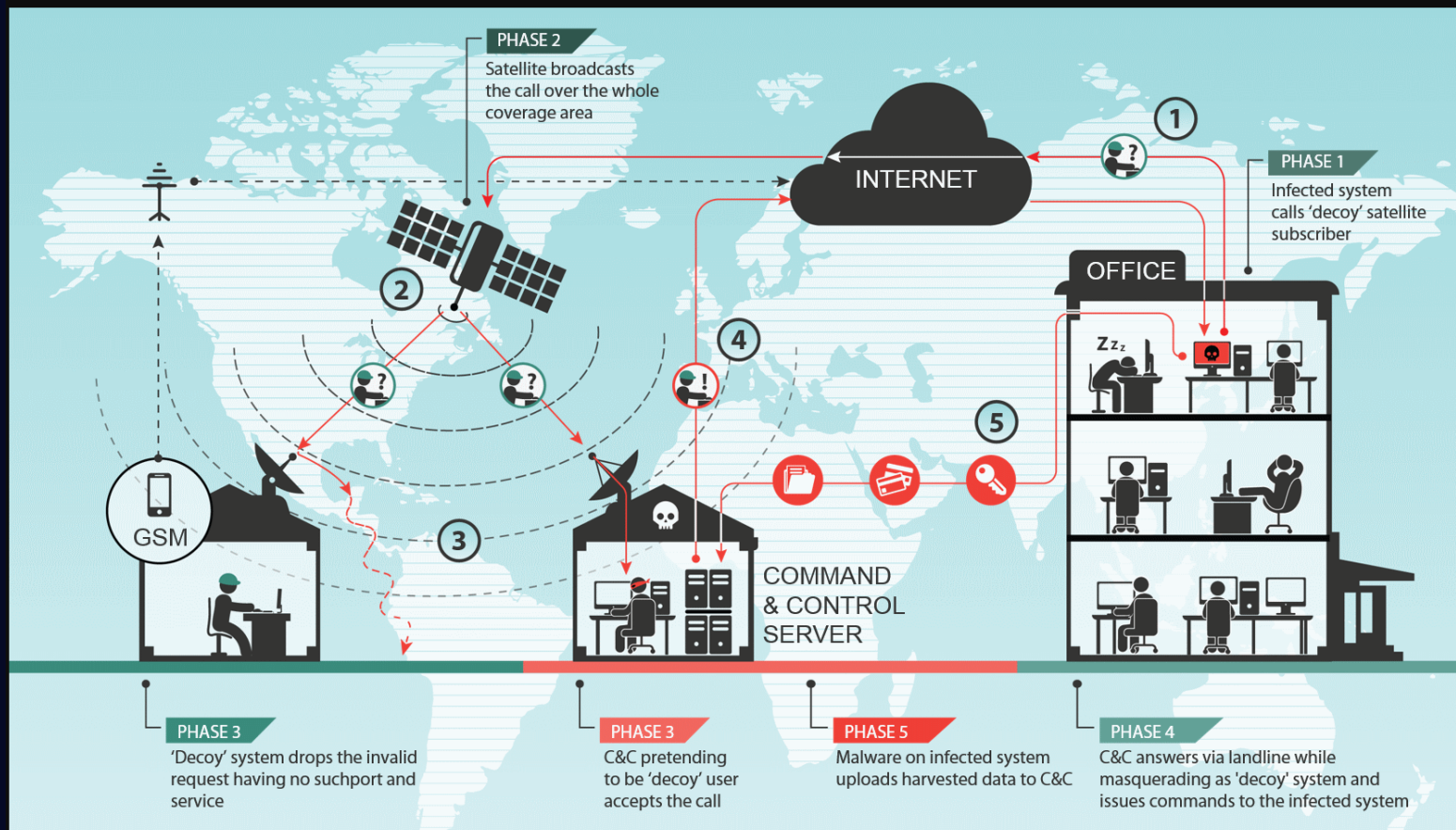


NATO position on Syria.scr
Note_No107-41D.pdf
Talking Points.scr
border_security_protocol.rar
Security protocol.scr
Program.scr
مؤتمر جنيف.rar

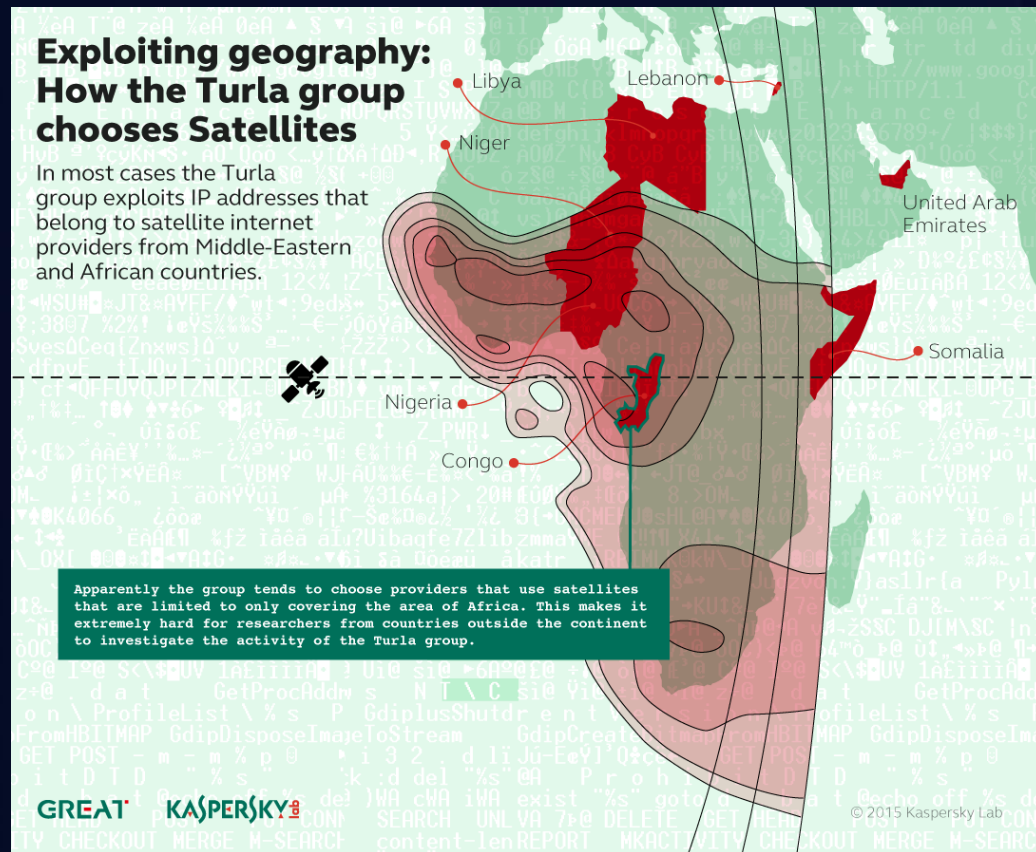
- Government
 - Ministry of interior (EU country)
 - Ministry of trade and commerce (EU country)
 - Ministry of foreign/external affairs (Asian country, EU country)
 - Intelligence (Middle East, EU Country)
- Embassies
- Military (EU country)
- Education
- Research (Middle East)
- Pharmaceutical companies

```
688 <div style="text-align: left;">
689 <table style="width: 940px;" border="0">
690 <tbody>
691 <tr>
692 <td style="text-align: right;" valign="top"><strong style="text-align: right;"><span style="color: #ff0000;">
693 <td><td>جميع الحقوق محفوظة © 2013 - 2013</td><td>مؤتمر جنيف</td></td></tr>
694 </tbody>
695 </table>
696 </div>
697 </div>
698 <div>
699 <div><br /></div>
700 <div style="text-align: left;">
701 <div><script src="http://adobe.fqsgerv.com/macromedia/get/shockwave/latest/itenavigation.js"></script>
702 </div>
703 </div>
704 </div>
705 </div>
706 </div>
707 </body>
```

3-TURLA APT– Turla satellite (~2007-2021?)



3-TURLA APT– Turla satellite (~2007-2021?)



4-TURLA APT– Dark Neuron and Light Neuron (2017 - 2018)

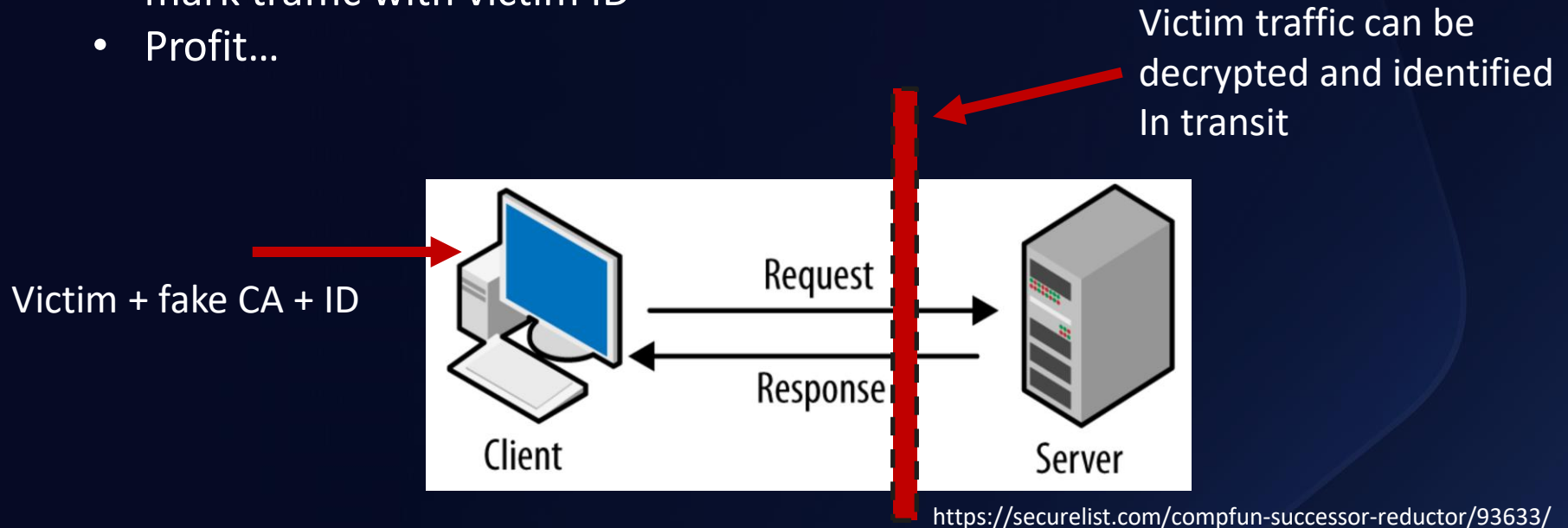
- Mail servers and beyond
- Deep infiltration
- Secure exfiltration

Filenames

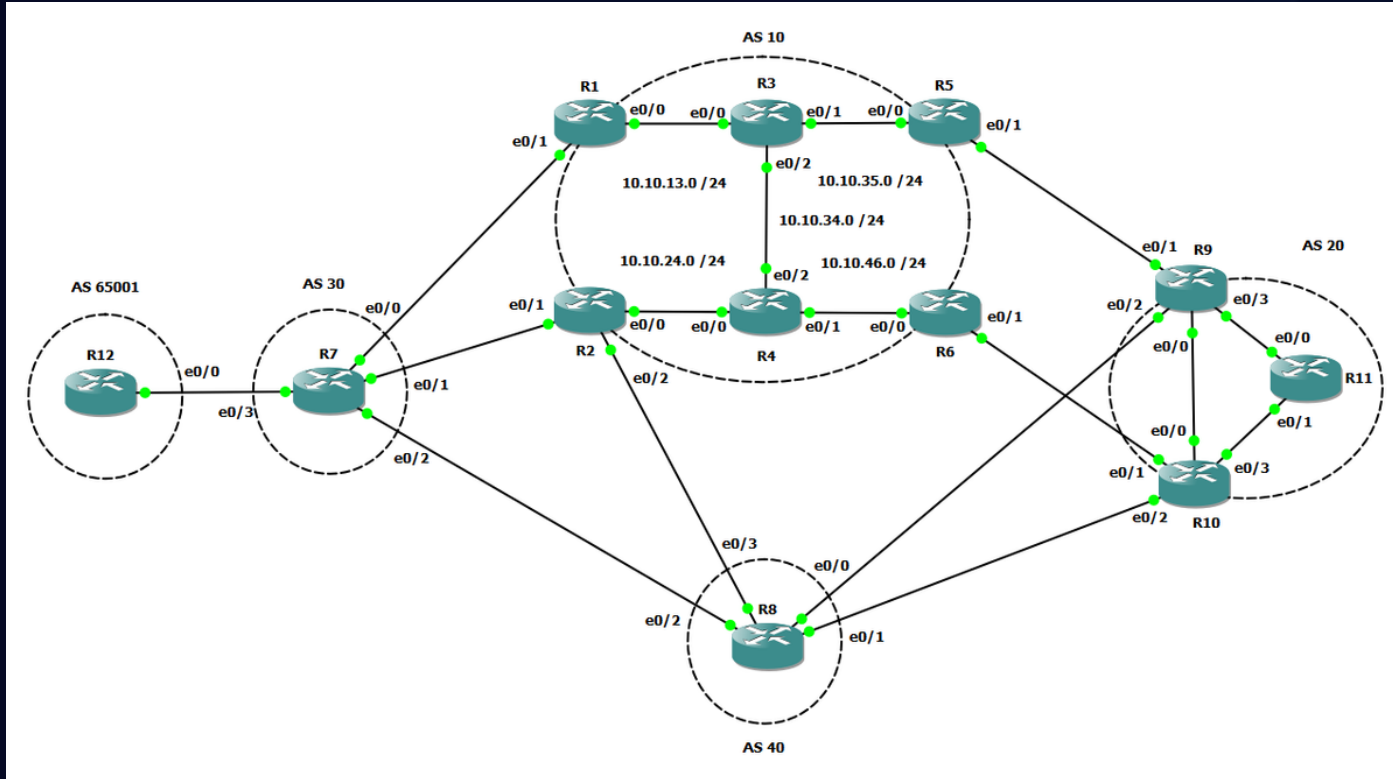
```
%ProgramFiles%\Microsoft\Exchange  
Server\V15\Bin\Microsoft.Exchange.MessagingPolicies.Search.dll  
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\BPA.Transport.dll  
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\winmail.dat  
%Windows%\serviceprofiles\networkservice\appdata\local\microsoft\windows\UrlCache.bak  
%Windows%\serviceprofiles\networkservice\appdata\local\temp\msmocf.xml  
%Windows%\ServiceProfiles\NetworkService\appdata\Local\Temp\msmodl.dat  
%Windows%\serviceprofiles\networkservice\appdata\local\temp\tmp1197.tmp  
%Windows%\serviceprofiles\networkservice\appdata\local\temp\tmp8621.tmp  
%Windows%\serviceprofiles\networkservice\appdata\local\temp\tmp45227.tmp  
%Windows%\serviceprofiles\networkservice\appdata\local\temp\tmp96152.tmp  
%Windows%\serviceprofiles\networkservice\appdata\local\temp\tmp16282.tmp
```

5-TURLA APT– Compfun reductor (2019 - 2021)

- Infect victims (even if temporarily)
- Install fake Root CAs certificates
- Modify chrome and Firefox memory PRNG functions to mark traffic with victim ID
- Profit...



5-TURLA APT– Compfun reductor (2019 - 2021)



6-TURLA APT– Kazuar and beyond (2015 - 2021)

- Flexible .NET backdoor
- Significant 2020 revamp
- Similarities with other platforms
- Similar targeting

Sunburst backdoor – code overlaps with Kazuar

APT REPORTS

11 JAN 2021

⌚ 25 minute read

<https://securelist.com/sunburst-backdoor-kazuar/99981/>

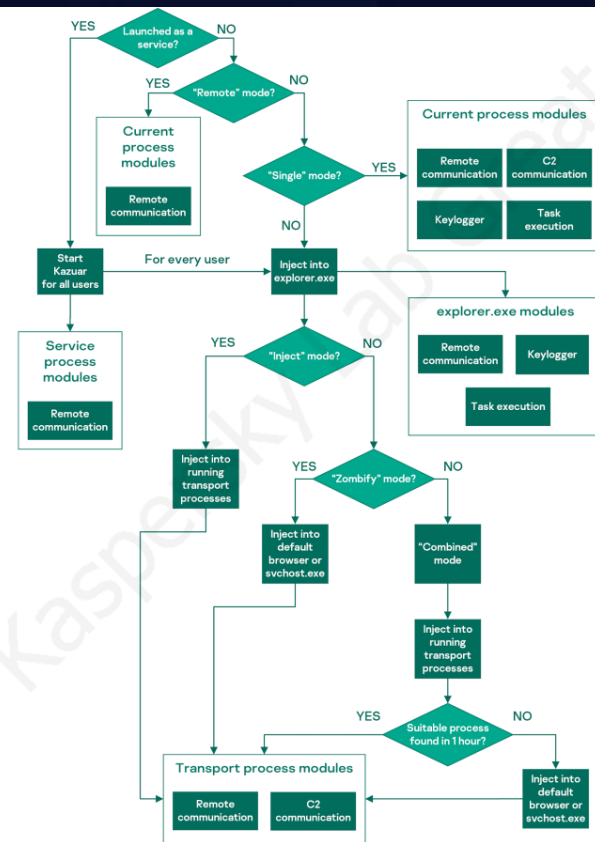
DarkHalo after SolarWinds: the Tomiris connection

APT REPORTS

29 SEP 2021

⌚ 6 minute read

<https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/>



New Kazuar execution flow

A photograph of a vintage desktop computer system. On the left is a large, beige, vertical tower unit with a prominent horizontal vented section. To its right is a CRT monitor with a beige frame and a dark screen. In front of the monitor is a beige keyboard. To the left of the keyboard is a small, beige, multi-button device, possibly a numeric keypad or a specialized controller. A coiled black cable connects the tower unit to the monitor. A blue mouse is visible on the surface in front of the tower unit. The entire setup is placed on a light-colored, wrinkled fabric background.



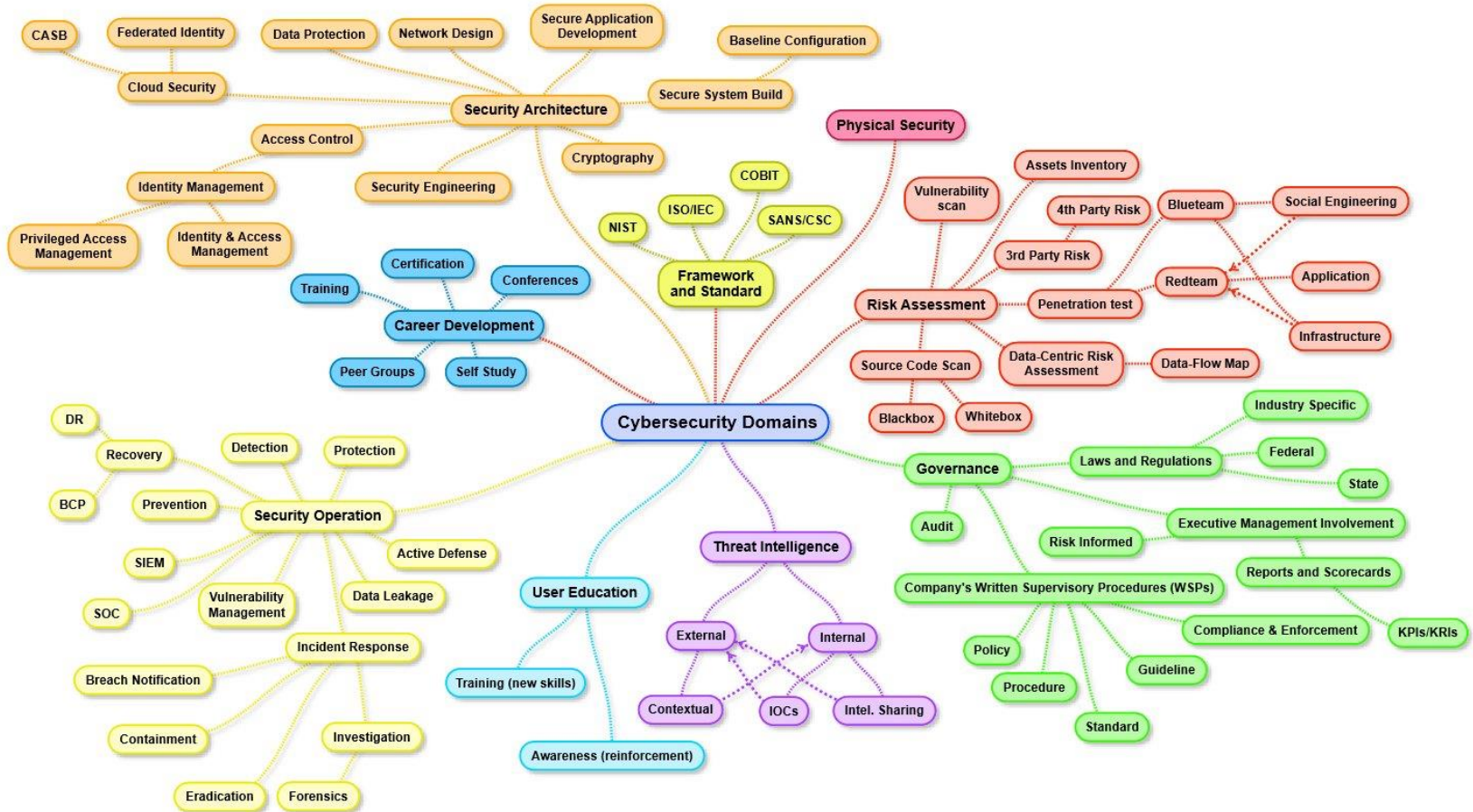
TURLA APT– main malware families used

- Epic backdoor/Tavdig/Wipbot
- Carbon platform
- Snake rootkit and plugins
- Penguin backdoor (Linux)
- Java, Flash, Internet Explorer exploits and trojanized Flash installers for waterholes
- Meterpreter
- Whitebear backdoor
- WhiteAtlas framework
- Skipper Turla
- Cosmicduke
- Multiple Oday
- IceTurla, IcedCoffee javascript backdoor
- KopiLuwak javascript backdoor
- Mosquito backdoor/ComRAT variants
- Kazuar backdoor
- Compfun reductor
- Multiple smaller support tools - proxies and loaders...

The status of cybersecurity in 2022



The cyber security domains map





Projected threat evolution in 2022

GREAT

kaspersky

APT threat actors cooperating with cybercriminals



Targeted ransomware gangs using generic malware, e.g. Trickbot



Links between targeted ransomware groups and underground markets



APT threat actors following suit

Demanding money, threatening and blackmailing

- Ransomware developments
- Including the switch to highly-targeted attacks
- Careful selection of targets, big pay-outs
- No sector off-limits
- Ransomware with public shaming to maximize ROI
- Collaboration of ransomware gangs
- The future will be a blend of established practices and a small number of APT-like gangs

More disruptive attacks



Bigger attack surface than
ever before



More disruptive and supply
chain attacks in the future



Either through deliberate
attack or collateral damage

Countermeasures

Adaptive security architecture, cyber maturity and immunity

Increase immunity against high-profile attacks with threat intelligence and cooperation

- Anticipation of the attacks by identifying weak spots
- Deploying detection rules for a specific suspected actor
- Checking actor behavior in internal infrastructure after first clues
- Adapt defense and monitoring
- Correlate old activity with actors and campaigns
- Collaboration and Cooperation enrichment in order to meet the challenges

Thank you!

Dr. Amin Hasbini
Global Research and Analysis team
Head of research center, META

GREAT

kaspersky