Mid-Atlantic CIO Forum

Secureworks®

Cybersecurity Technologies. Services. Solutions.

Ryan Alban, CISSP | GISP

Sr. Manager,
Global Solution Leads,
Threat Detection and Response

in™

CISSP®

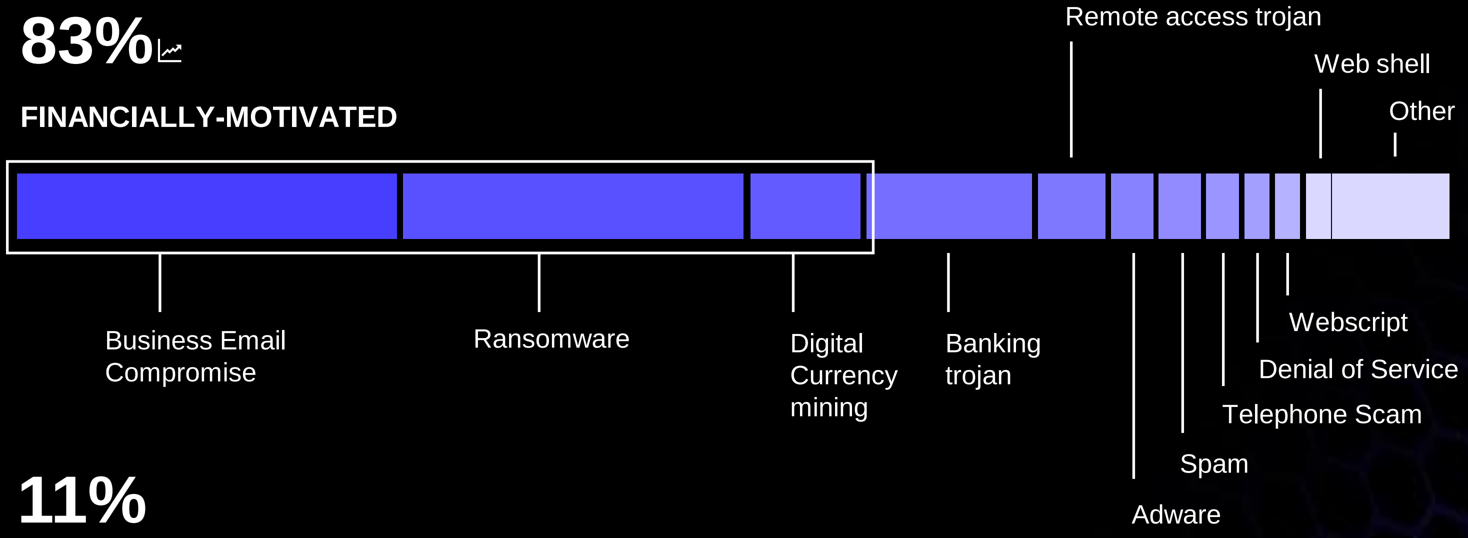
GISP

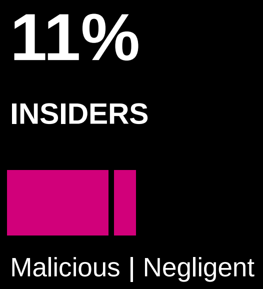
Incident Response Trends and Analyses

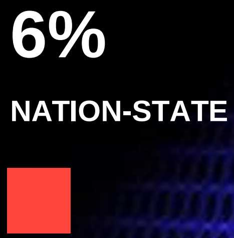
83%

of incidents SCWX investigated in Q2-2020 were financially-motivated.

Q2 2020 Threats as Observed Through IR





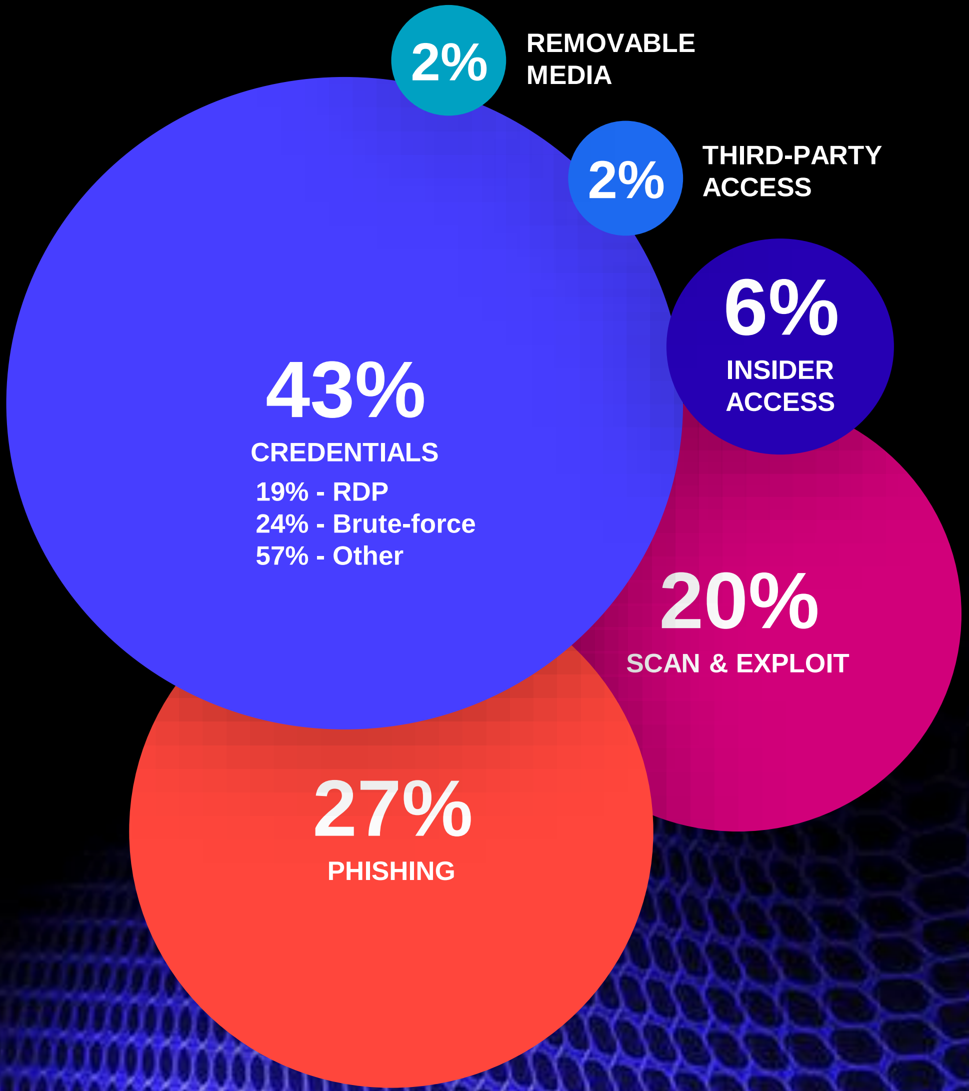


Incident Response Trends and Analyses

43%

of incidents SCWX investigated in Q2 2020 began with compromised credentials.

How are they getting in?



Ransomware as a Service Market Landscape

2005

The year SCWX analyzed the first known ransomware threat.

Fierce Competition

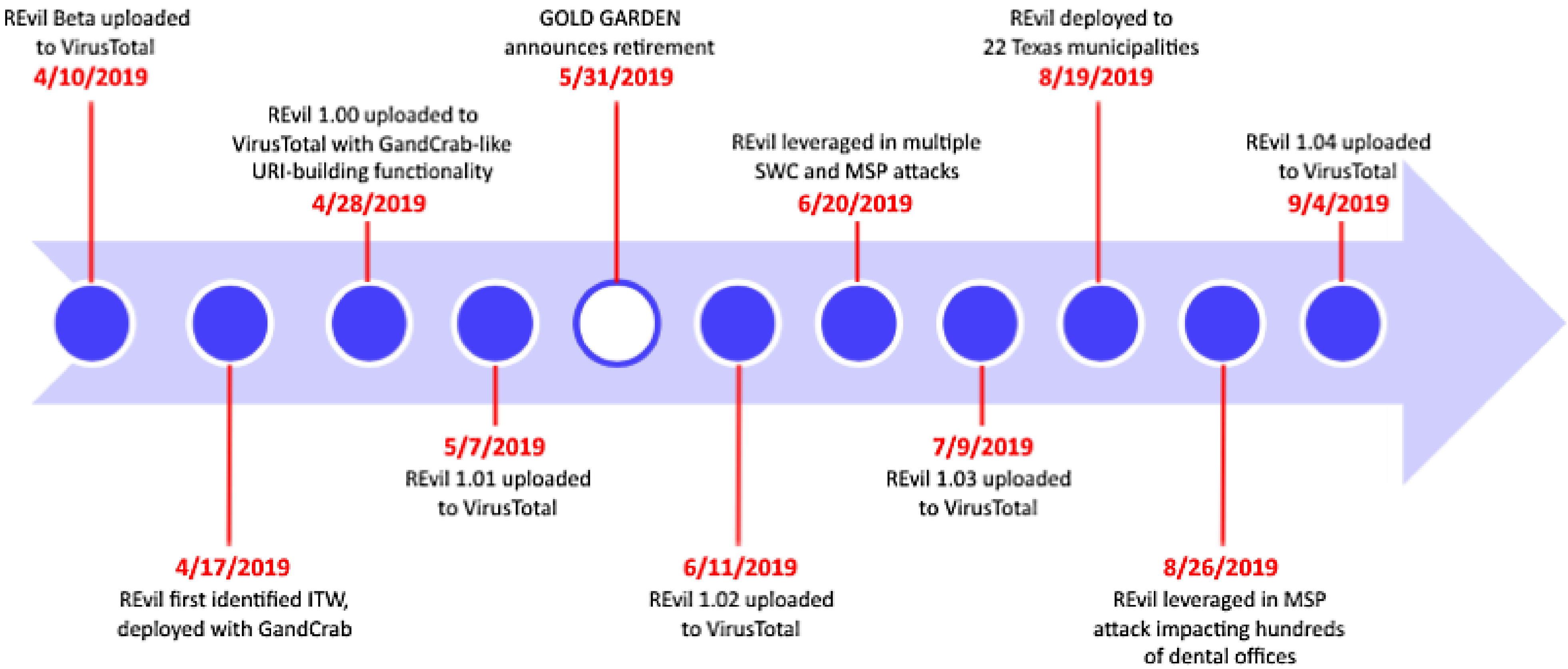
The RaaS Market is Complex and Competitive

Image Removed for Distribution

[REvil/Sodinokibi Ransomware | Secureworks]()

Robust Agile Development Sprints

The cadence by which GOLD SOUTHFIELD released new REvil versions (see Figure 1) indicated a structured process by experienced malware developers. On October 7, CTU(TM) researchers identified REvil 1.05. The timing of this version adheres to the monthly release pattern.



REvil Beta uploaded to VirusTotal
4/10/2019

4/17/2019
REvil first identified ITW, deployed with GandCrab

REvil 1.00 uploaded to VirusTotal with GandCrab-like URI-building functionality
4/28/2019

5/7/2019
REvil 1.01 uploaded to VirusTotal

GOLD GARDEN announces retirement
5/31/2019

6/11/2019
REvil 1.02 uploaded to VirusTotal

REvil leveraged in multiple SWC and MSP attacks
6/20/2019

7/9/2019
REvil 1.03 uploaded to VirusTotal

REvil deployed to 22 Texas municipalities
8/19/2019

8/26/2019
REvil leveraged in MSP attack impacting hundreds of dental offices

REvil 1.04 uploaded to VirusTotal
9/4/2019

REvil Ransomware: The GandCrab Connection | Secureworks

Mergers and Acquisitions

…Unknown's claims, if true, present a scenario where an affiliate gains experience within a RaaS environment, builds rapport with an advanced threat group, convinces the threat group to sell its code, and then splits from the threat group to build a distinct RaaS offering

Image Removed for Distribution

[Ransomware is the Number One Cyber Threat to Organizations Today | Secureworks]()

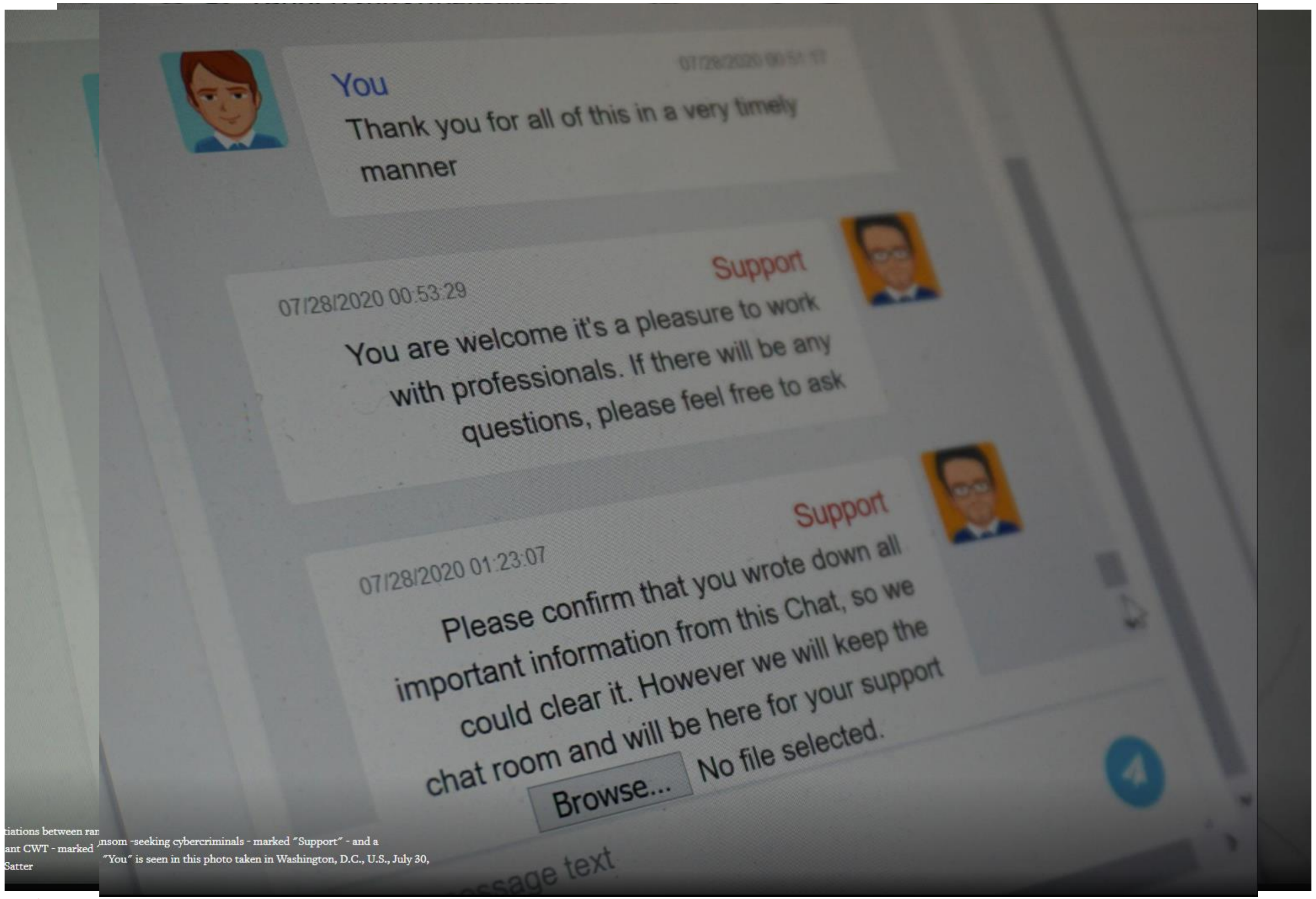
Channel Programs and Affiliate Business Models

Image Removed for Distribution

Netwalker ransomware earned $25 million in just five months (bleepingcomputer.com)

Customer Support

Prompt and courteous service is a differentiator…



You 07/28/2020 00:51:17
Thank you for all of this in a very timely manner

07/28/2020 00:53:29 Support
You are welcome it's a pleasure to work with professionals. If there will be any questions, please feel free to ask

07/28/2020 01:23:07 Support
Please confirm that you wrote down all important information from this Chat, so we could clear it. However we will keep the chat room and will be here for your support

tiations between ran
ant CWT - marked
Satter

nsom -seeking cybercriminals - marked "Support" - and a
"You" is seen in this photo taken in Washington, D.C., U.S., July 30,

https://www.reuters.com/article/us-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-4-5-million-ransom-to-cyber-criminals-idUSKCN24W25W

Call to action.

Prevention Recommendations from Incident Response Team

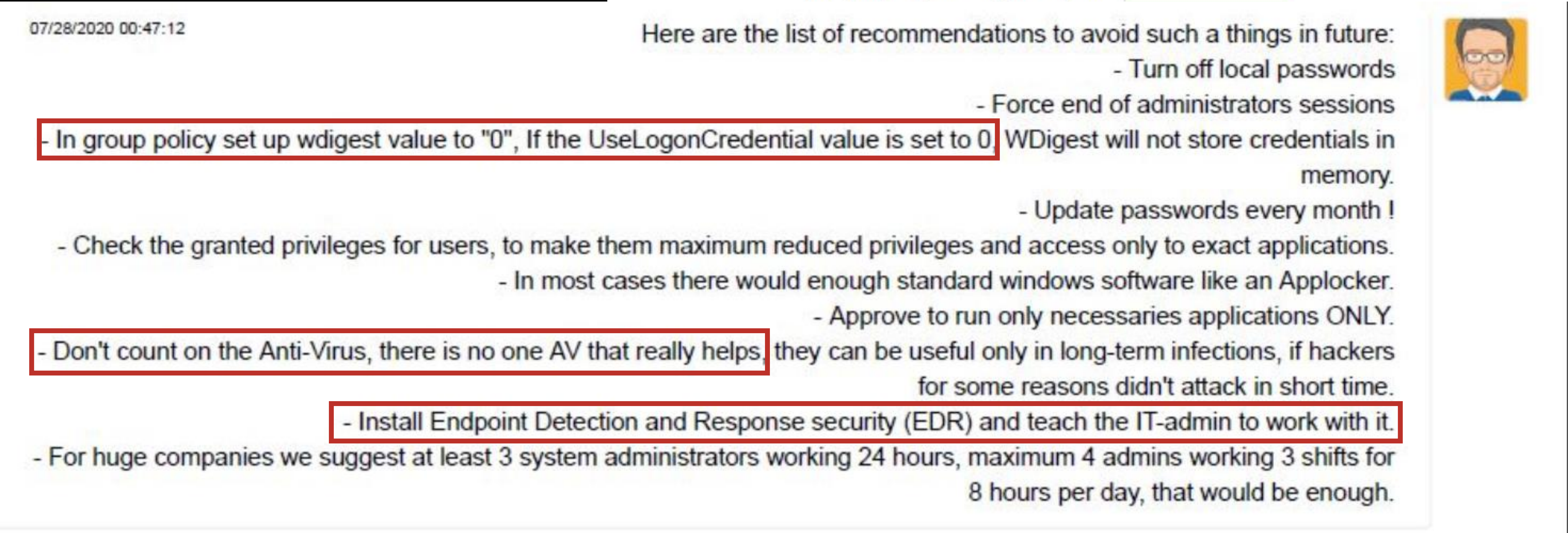
Implement Multi-Factor Authentication

Image Removed for Distribution

Secureworks 2019 Incident Response Insights Report | Secureworks

Detection Recommendations from ~~Incident Response Team~~

Ragnar Locker Operators



07/28/2020 00:47:12

Here are the list of recommendations to avoid such a things in future:
- Turn off local passwords
- Force end of administrators sessions
- In group policy set up wdigest value to "0", If the UseLogonCredential value is set to 0, WDigest will not store credentials in memory.
- Update passwords every month !
- Check the granted privileges for users, to make them maximum reduced privileges and access only to exact applications.
- In most cases there would enough standard windows software like an Applocker.
- Approve to run only necessaries applications ONLY.
- Don't count on the Anti-Virus, there is no one AV that really helps, they can be useful only in long-term infections, if hackers for some reasons didn't attack in short time.
- Install Endpoint Detection and Response security (EDR) and teach the IT-admin to work with it.
- For huge companies we suggest at least 3 system administrators working 24 hours, maximum 4 admins working 3 shifts for 8 hours per day, that would be enough.

iTWire - Big US travel management firm CWT pays out US$4.5m to

Response Recommendations from Incident Response Team

Reset Compromised Account Credentials

Image Removed for Distribution

[Secureworks 2019 Incident Response Insights Report | Secureworks]

thank you.