GARMIN™


Map
Back
Menu
Direct To
Zoom In
Zoom Out


This Week 30.0 mi
10.65
1:08:20
6:25/mi
GARMIN


GPSMAP
GARMIN

Garmin Ransomware Attack

- Occurred on July 23, 2020
- Garmins systems rendered useless, such as Garmin Connect, and flyGarmin
- Evil Corp was behind the attack, and utilized the WastedLocker ransomware
- Evil Corp requested a $10 million ransom to release control of Garmin’s systems

Evil Corp

- Russian hacker group behind the attack
- A 5 million dollar reward is given to anyone with information leading leading to the arrest of the leader of Evil Corp
  - This is the largest ever for a cyber criminal

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

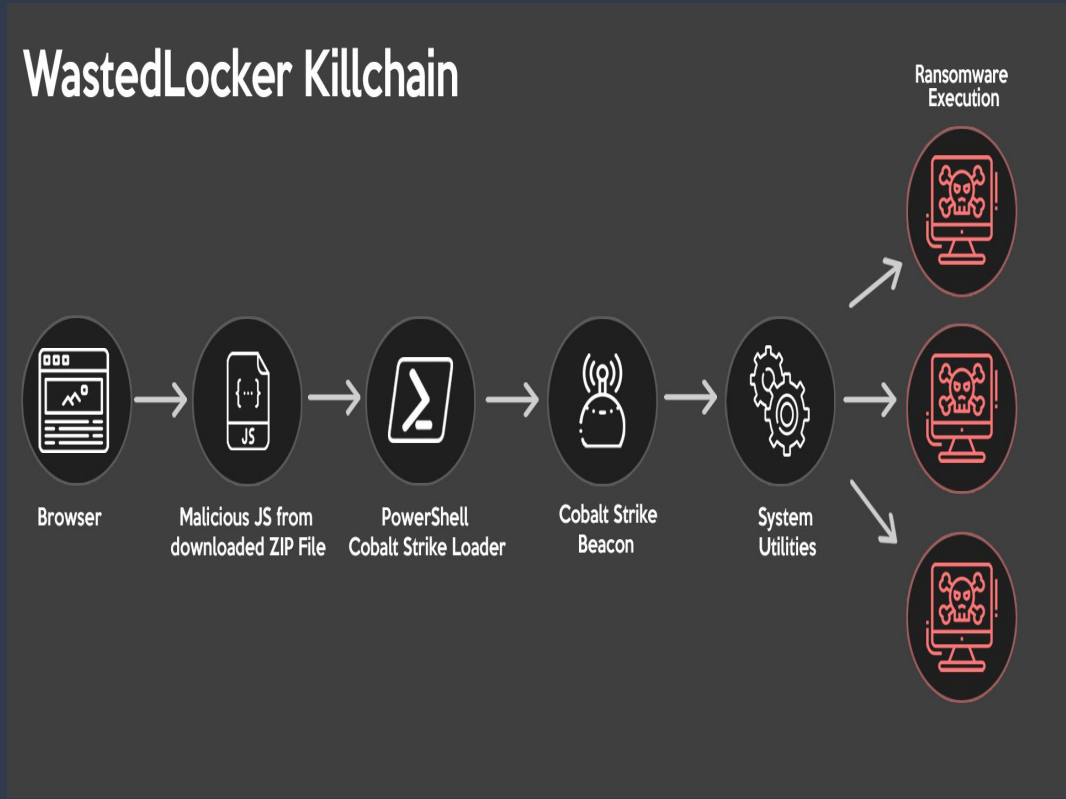
Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

WastedLocker

- The ransomware used for the attack
- Goal of WastedLocker is to encrypt all the files in a victim's system, and make the victim pay for the decryption key
- End goal is not to steal and sell the victim's data



Technical Analysis

Overview of Attack:

- Victim visits compromised website, downloads a zipped file containing malicious JavaScript that is hidden in a fake browser update, deployed via the SocGholish framework
- Cobalt Strike deployed on the infected system, allows attacker to move along the infected network
- Attacker elevates their privileges using a UAC bypass
- Attacker then encrypts most of the files on the system

Technical Analysis

Command Line Arguments:

- -p <directory-path> or -f<directory-path>
  - prioritizes a certain directory before encrypting others or only encrypts that specific directory
- -u username:password\\hostname (Attacker must enter these credentials)
- -r
  - deletes any shadow copies of the directory files
  - Copies ransomware binary to %windir%\system32 and resets ACL permissions
  - Creates and runs the service then deletes the service once complete
- -s
  - starts executing the service (starts the encryption process)

Technical Analysis

Cobalt Strike

- Commercially available software used for white hat security testing
- One feature allows user to download and execute code on target network
- Hackers use its features to deliver WastedLocker’s malware

Technical Analysis

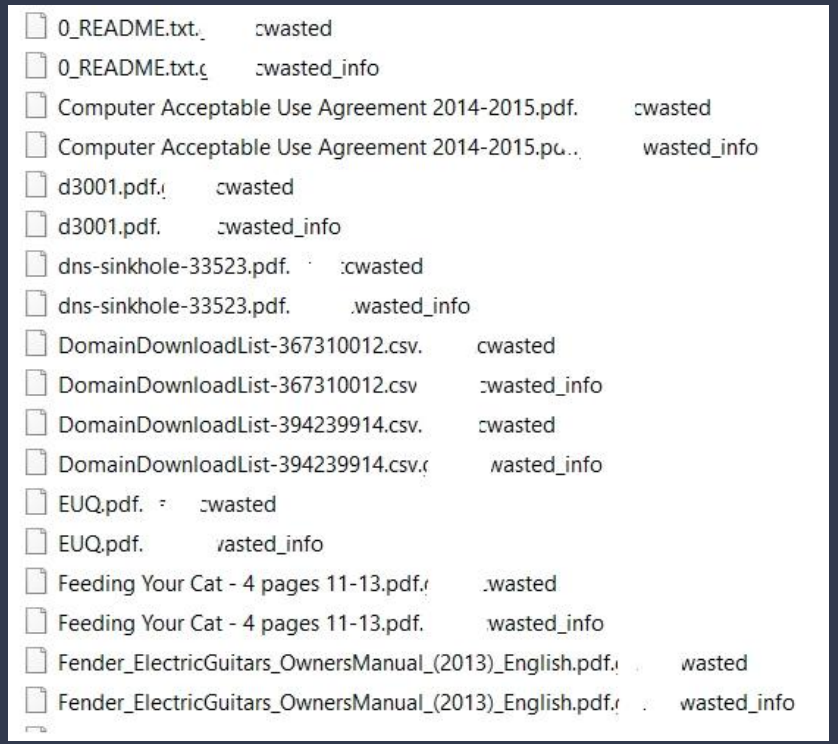
Gaining Administrative Access

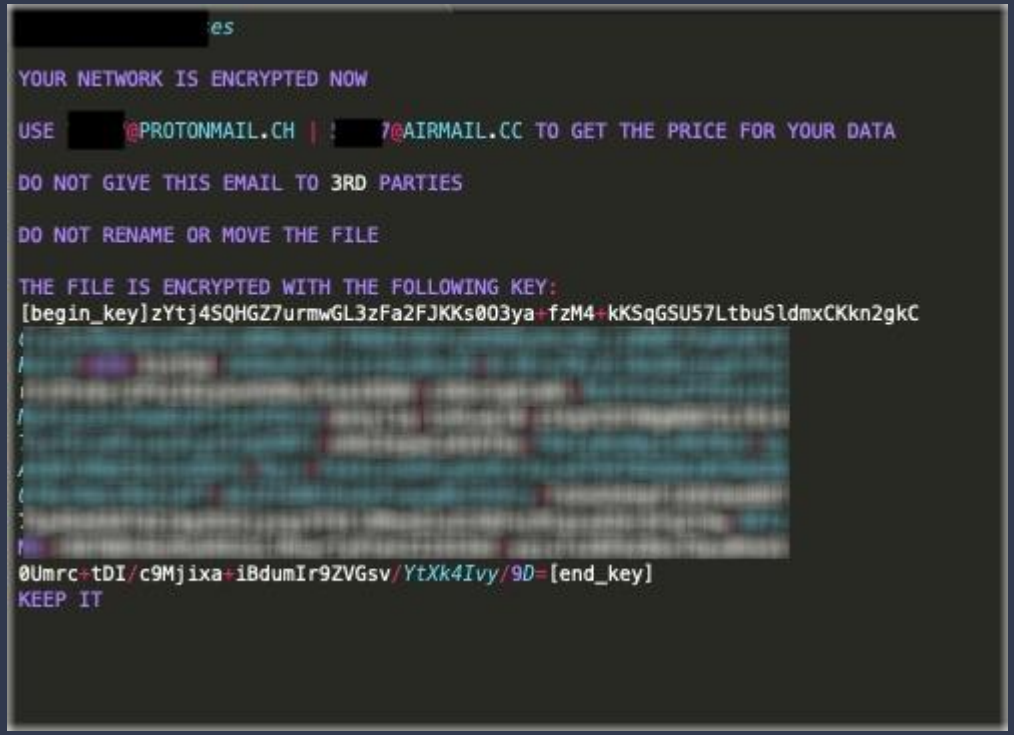
- Normally Windows UAC blocks/warns of malicious software
- WastedLocker bypasses UAC using a fake system32 directory
- Copies winsat.exe and winmm.dll to directory, patches winmm.dll to redirect to the malware
- Launching winsat.exe loads winmm.dll, which runs WastedLocker with elevated privelage

Technical Analysis

Encryption

- All files larger than 10 bytes are encrypted
- First encrypted with with 256 bit AES key and an Installation Vector (IV)
  - AES key is the SHA 256 hash of a particular string
  - IV is created from malware itself
- Then AES key / IV is further encrypted with a public RSA 4096 key
- Larger files are split into 64 mb blocks



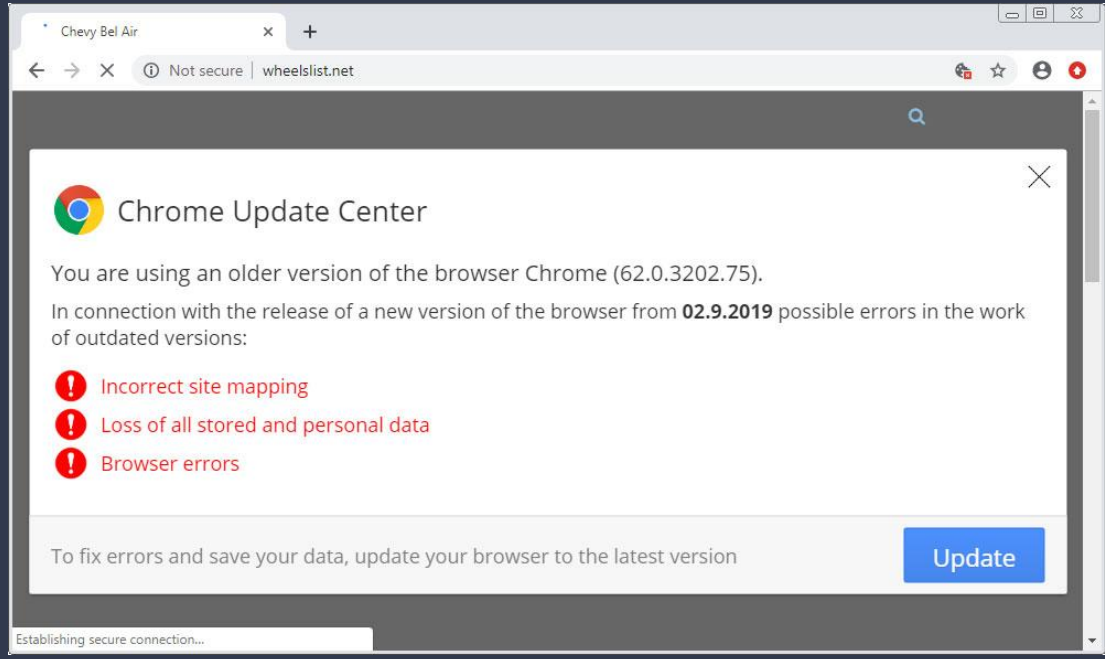


For each file:

- Filename.wasted is the encrypted file
- Filename.wasted_info is the ransom note

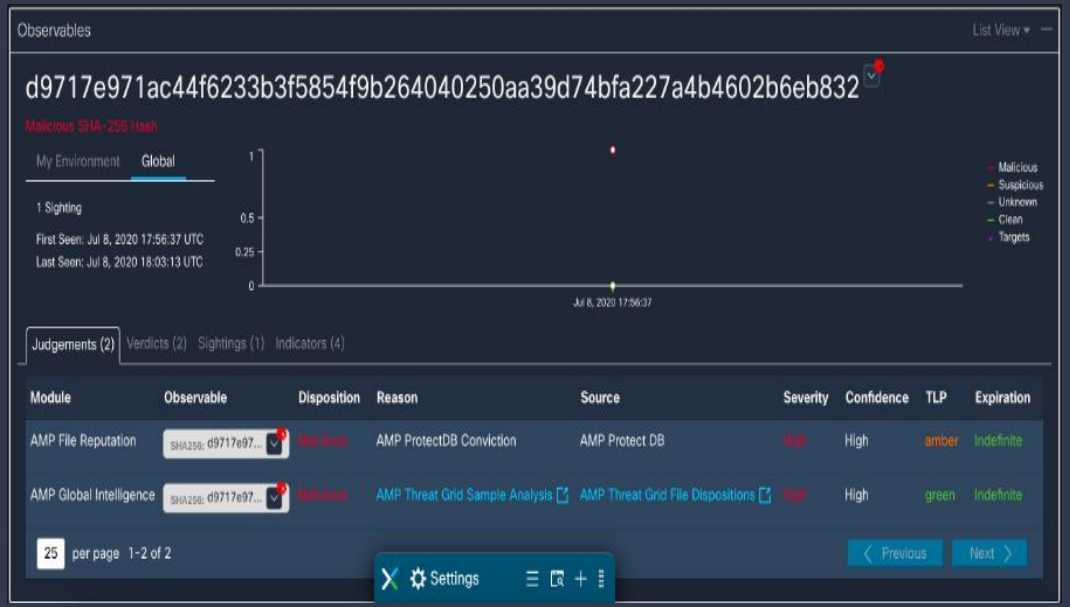
Prevention

- Better training for employees to recognize signs of potential attack
  - The first part of the attack is getting the victim to run a fake browser update that contains malware



Prevention

- Implementing products into the system that can recognize and prevent this attack
- Cisco offers multiple products to prevent the WastedLocker ransomware
  - Cisco Umbrella
  - AMP for Endpoints
  - Cisco Stealthwatch



Incentives

Why perform a Ransomware attack?

- Hold company data “hostage” so that the company will pay attackers a lot of money

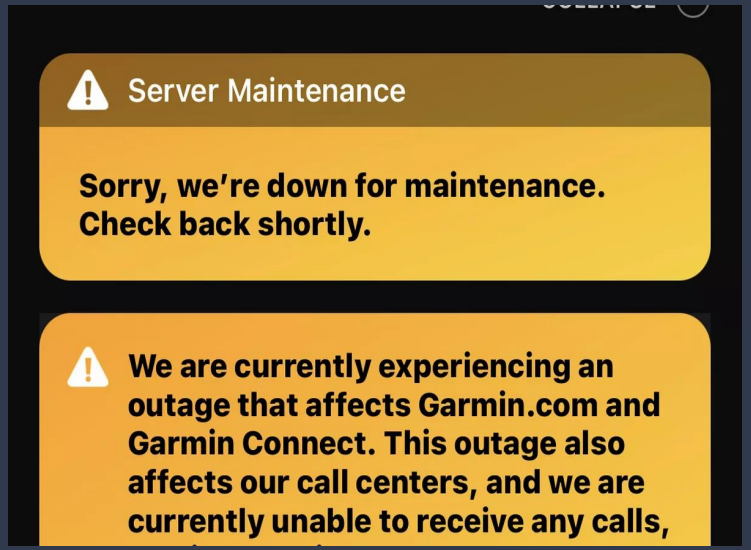
Why target Garmin?

- Big Corporation so they have a lot of $
- Have mission-critical data
- The attack would impact customers so it puts more pressure on Garmin

Incentives

How was Garmin affected?

- Garmin was forced offline for 5 days
- Garmin fitness activity uploads were down
- FlyGarmin navigation service for aviation was also affected
- No data was stolen



Incentives

Why was Garmin attacked at that specific date (July 23, 2020)?

- Attack was right before quarterly earnings were to be reported (July 29, 2020)
- Increases likelihood of payout
- Garmin doesn’t want their financial data to be affected
- Garmin saw overall 9% decline in revenue in quarter 2

Ethics

Should Victims Pay Ransom?

- Not simple to answer
- Lose/Lose situation

If They Pay

- Demonstrates lack of defenses
- Motivates future attacks on victim and other organizations

If They Refuse

- Loses data
- Sometimes stakes are too high to refuse (e.g. human life)

Legal Matters

Computer Fraud and Abuse Act (CFAA)

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),[4] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

State Level

- California and Wyoming
  - Have laws put in place specifically for ransomware
  - Max of 10 years in jail, $10,000 fine or both
- Maryland
  - Tried creating a similar law, not passed

Executive Order 13694

Signed by President Obama on April 1st 2015
Allows sanctions against individuals/groups that are or help groups that threaten one of the following of the US

- National security
- Foregin policy
- Economic health
- Financial stability

Evil Corp Sanctioned 2015

Punishments for Violating Sanctions

- Fines up to $20 Million
- Prison sentences up to 30 years

If also convicted of “Trading with the Enemy”

- Up to $65,000 per conviction

If violates International Emergency Economic Power Act

- Up to $250,000 per violation

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer




DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

CAUTION

Maksim Viktorovich Yakubets is wanted for his involvement with computer malware that infected tens of thousands of computers in both North America and Europe, resulting in actual financial losses in the tens of millions of dollars.

Specifically, Yakubets was involved in the installation of malicious software known as Zeus, which was disseminated through phishing emails and used to capture victims' online banking credentials. These credentials were then used to steal money from the victims' bank accounts. On August 22, 2012, an individual was charged in a superseding indictment under the moniker "aqua" in the District of Nebraska with conspiracy to participate in racketeering activity, conspiracy to commit computer fraud and identity theft, aggravated identity theft, and multiple counts of bank fraud. On November 14, 2019, a criminal complaint was issued in the District of Nebraska that ties the previously indicted moniker of "aqua" to Yakubets and charges him with conspiracy to commit bank fraud.

Yakubets is also allegedly the leader of the Bugat/Cridex/Dridex malware conspiracy wherein he oversaw and managed the development, maintenance, distribution, and infection of the malware. Yakubets allegedly conspired to disseminate the malware through phishing emails, to use the malware to capture online banking credentials, and to use these captured credentials to steal money from the victims' bank accounts. He, subsequently, used the malware to install ransomware on victims' computers. Yakubets was indicted in the Western District of Pennsylvania, on November 13, 2019, and was charged with Conspiracy, Conspiracy to Commit Fraud, Wire Fraud, Bank Fraud, and Intentional Damage to a Computer.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Offices: Omaha, Pittsburgh

www.fbi.gov

WANTED BY THE FBI

IGOR OLEGOVICH TURASHEV

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

ki, Parasurama, Nintutu, Vzalupkin, Tigrr, Tigrruz

Birth Used: June 15, 1981	**Place of Birth:** Yoshkar-Ola, Russia
roximately 5'10"	**Eyes:** Brown
	Sex: Male
	Nationality: Russian

CAUTION

Turashev is wanted for his involvement with computer malware which infected tens of thousands n both North America and Europe, resulting in financial losses in the tens of millions of dollars. dly handled a variety of responsibilities for the Bugat/Cridex/Dridex malware conspiracy including tration, management of internal control panels, and oversight of the botnet operations. He allegedly iseminate the malware through phishing emails, to use the malware to capture online banking l to use these captured credentials to steal money from the victims' bank accounts. He, subsequently, re to install ransomware on victims' computers.

dicted in the Western District of Pennsylvania, on November 13, 2019, and was charged with spiracy to Commit Fraud, Wire Fraud, Bank Fraud, and Intentional Damage to a Computer.

information concerning this person, please contact your local FBI office or the nearest ssy or Consulate.

sburgh

www.fbi.gov

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

Cracks Down on Groups Making Ransomware Payments Through 3rd Parties to Avoid Sanctions Like What Garmin Did