WastedLocker: technical analysis

By Fedor Sinitsyn

Published: 2020-07-31 · Archived: 2026-04-05 13:35:24 UTC

The use of crypto-ransomware in targeted attacks has become an ordinary occurrence lately: new incidents are being reported every month, sometimes even more often.

On July 23, Garmin, a major manufacturer of navigation equipment and smart devices, including smart watches and bracelets, experienced a massive service outage. As confirmed by an official statement later, the cause of the downtime was a cybersecurity incident involving data encryption. The situation was so dire that at the time of writing of this post (7/29) the operation of the affected online services had not been fully restored.

According to currently available information, the attack saw the threat actors use a targeted build of the trojan WastedLocker. An increase in the activity of this malware was noticed in the first half of this year.

We have performed technical analysis of a WastedLocker sample.

Command line arguments

It is worth noting that WastedLocker has a command line interface that allows it to process several arguments that control the way it operates.

-p <directory-path>

Priority processing: the trojan will encrypt the specified directory first, and then add it to an internal exclusion list (to avoid processing it twice) and encrypt all the remaining directories on available drives.

-f <directory-path>

Encrypt only the specified directory.

-u username:password \\hostname

Encrypt files on the specified network resource using the provided credentials for authentication.

-r

Launch the sequence of actions:

1. 1 Delete ;
2. 2 Copy to %WINDIR%\system32\<rand>.exe using a random substring from the list of subkeys of the registry key SYSTEM\CurrentControlSet\Control\;
3. 3 Create a service with a name chosen similarly to the method described above. If a service with this name already exists, append the prefix “Ms” (e.g. if the service “Power” already exists, the malware will create a

new one with the name “MsPower”). The command line for the new service will be set to “%WINDIR%\system32\<rand>.exe -s”;
4. 4 Start this service and wait until it finishes working;
5. 5 Delete the service.

-s:

Start the created service. It will lead to the encryption of any files the malware can find.

UAC bypass

Another interesting feature of WastedLocker is the chosen method of UAC bypass. When the trojan starts, it will check the integrity level it was run on. If this level is not high enough, the malware will try to silently elevate its privileges using a known bypass technique.

1. 1 Create a new directory in %appdata%; the directory name is chosen at random from the substrings found in the list of subkeys of the registry key SYSTEM\CurrentControlSet\Control\;
2. 2 Copy a random EXE or DLL file from the system directory to this new directory;
3. 3 Write the trojan’s own body into the alternate NTFS stream “:bin” of this system file;
4. 4 Create a new temporary directory and set its mount point to “C:\Windows ” (with a trailing whitespace) using the API function NtFsControlFile with the flag IO_REPARSE_TAG_MOUNT_POINT;
5. 5 Create a new subdirectory named “system32” inside the temporary directory. As a result of the previous step, this new subdirectory can be equally successfully addressed as “%temp%\ <directory_name>\system32” or “C:\Windows \system32” (note the whitespace);
6. 6 Copy the legitimate winsat.exe and winmm.dll into this subdirectory;
7. 7 Patch winmm.dll: replace the entry point code with a short fragment of malicious code whose only purpose is to launch the content of the alternate NTFS stream created on step 2;
8. 8 Launch winsat.exe, which will trigger the loading of the patched winmm.dll as a result of DLL hijacking.

The above sequence of actions results in WastedLocker being relaunched from the alternate NTFS stream with elevated administrative privileges without displaying the UAC prompt.

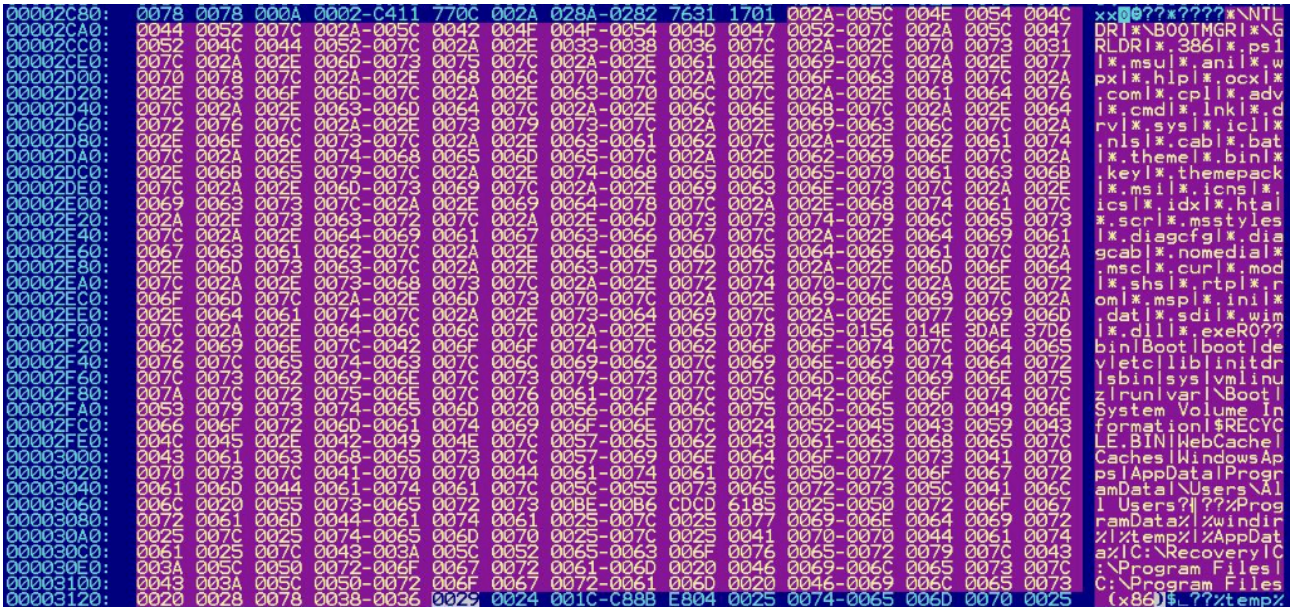
1768	CreateFile	C:\Windows	SUCCESS	Desired Access: Generic Write, Disposition: OpenIf, Options: Dire
1768	FileSystemControl	C:\Windows	SUCCESS	Control: FSCTL_SET_REPARSE_POINT
1768	CreateFile	C:\Windows	REPARSE	Desired Access: Read Data/List Directory, Synchronize, Disposit
1768	Process Create	C:\Windows \system32\winsat.exe	SUCCESS	PID: 4344, Command line: "C:\Windows \system32\winsat.exe"
1768	FileSystemControl	C:\Windows	SUCCESS	Control: FSCTL_DELETE_REPARSE_POINT
1768	CloseFile	C:\Windows	SUCCESS	

Procmon log fragment during the launch of WastedLocker

Cryptographic scheme

To encrypt victims’ files, the developers of the trojan employed a combination of the AES and RSA algorithms that has already become a ‘classic’ among different crypto-ransomware families.

The search mask to choose which files will be encrypted, as well as the list of the ignored paths are set in the configuration of the malware.



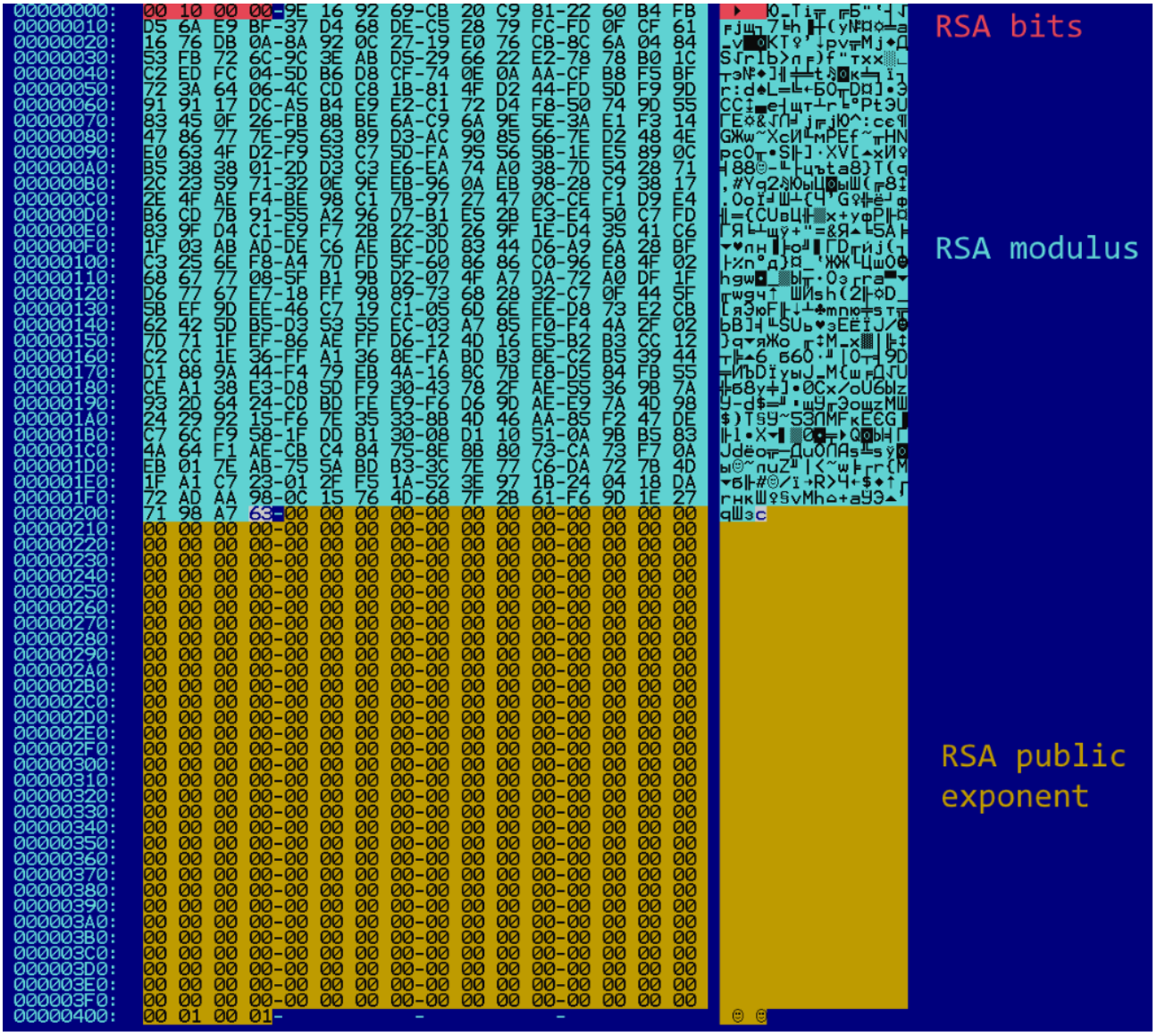
Part of the trojan config showing the ignored path substrings

For each processed file, WastedLocker generates a unique 256 bit key and a 128 bit IV which will be used to encrypt the file content using the AES-256 algorithm in CBC mode. The implementation of the file operations is worthy of note, as it employs file mapping for data access. It must have been an attempt by the criminals to maximize the trojan's performance and/or avoid detection by security solutions. Each encrypted file will get a new additional extension: "**.garminwasted**".

The trojan also implements a way of integrity control as part of its file encryption routine. The malware calculates an MD5 hash of the original content of each processed file, and this hash may be utilized during decryption to ensure the correctness of the procedure.

WastedLocker uses a publicly available reference implementation of an RSA algorithm named "rsaref".

The AES key, IV and the MD5 hash of the original content, as well as some auxiliary information, are encrypted with a public RSA key embedded in the trojan's body. The sample under consideration contains a 4096 bit public RSA key.

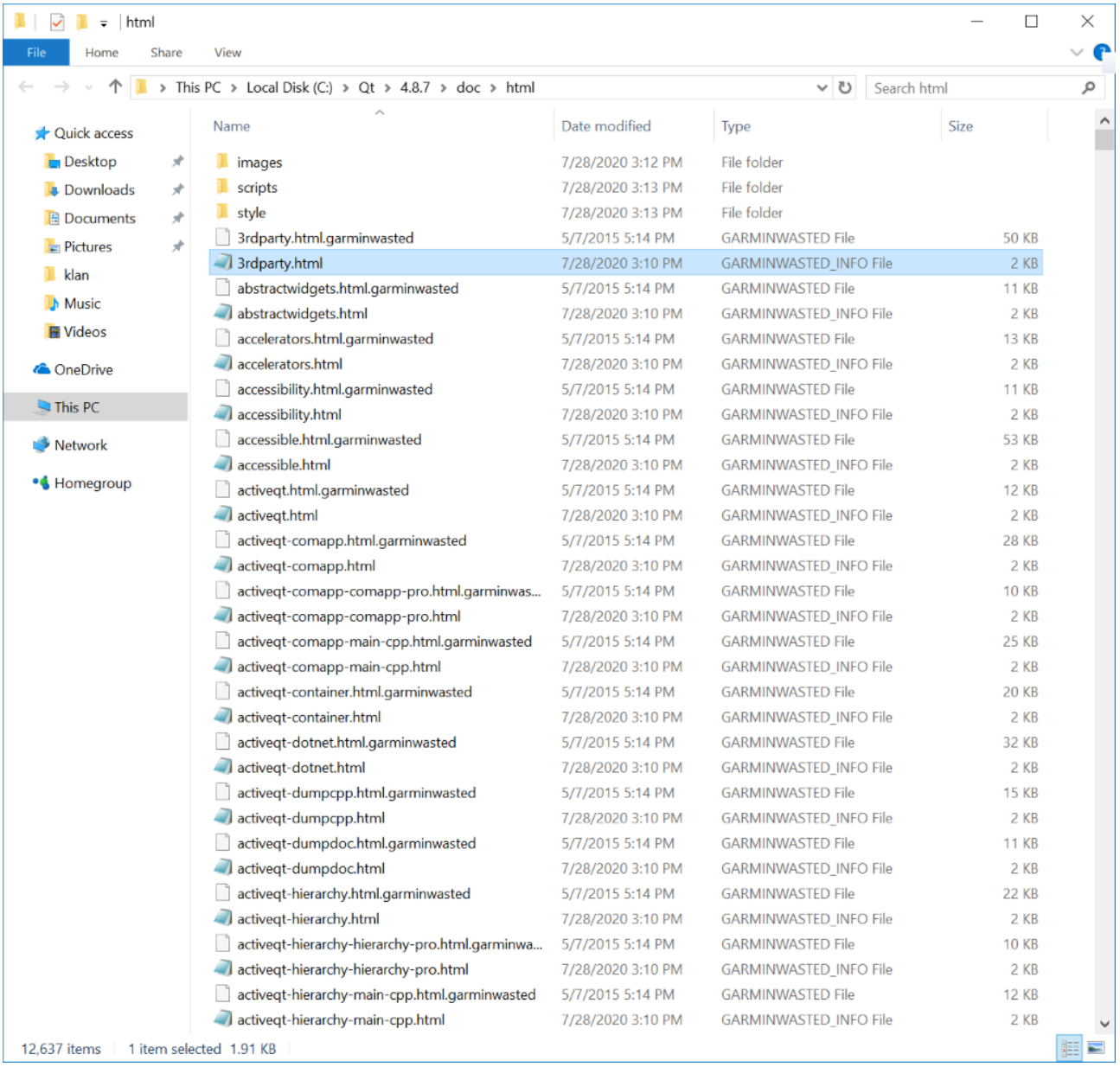


The public RSA key format used by WastedLocker

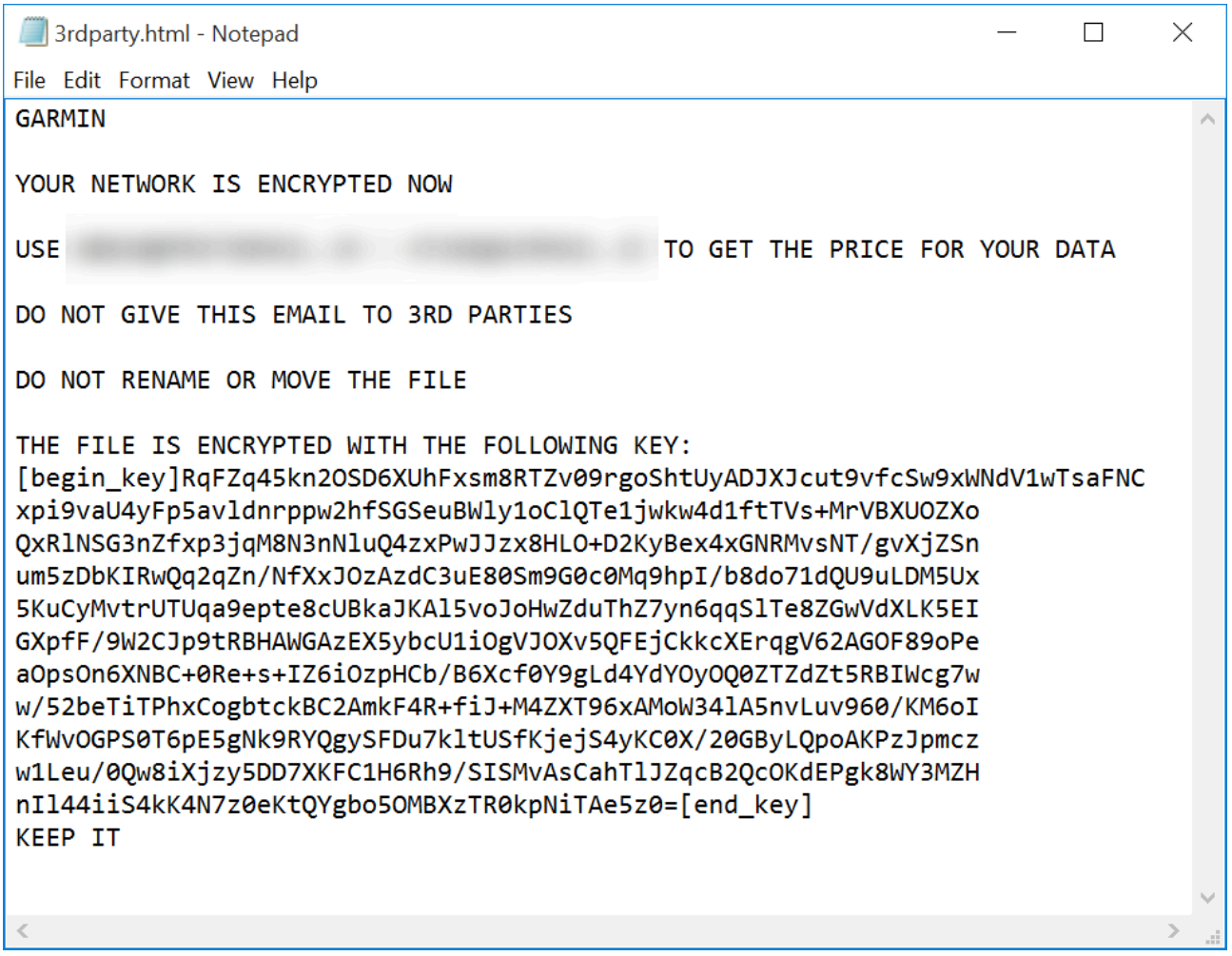
It should be noted that this kind of cryptographic scheme, using one public RSA key for all victims of a given malware sample, could be considered a weakness if WastedLocker were to be mass-distributed. In this case a decryptor from one victim would have to contain the only private RSA key that would allow all the victims to decrypt their files.

However, as we can see, WastedLocker is used in attacks targeted at a specific organization which makes this decryption approach worthless in real-world scenarios.

The result of RSA encryption is Base64 encoded and saved in a new file with the extension **.garminwasted_info**, and what is notable, a new info file is created for each of the victim's encrypted files. This is a rare approach that was previously used by the BitPaymer and DoppelPaymer trojans.



An example list of encrypted files from our test machine



Ransom note left by the trojan

Recommendations

This WastedLocker sample we analyzed is targeted and crafted specifically to be used in this particular attack. It uses a “classic” AES+RSA cryptographic scheme which is strong and properly implemented, and therefore the files encrypted by this sample cannot be decrypted without the threat actors’ private RSA key.

The Garmin incident is the next in a series of targeted attacks on large organizations involving crypto-ransomware. Unfortunately, there is no reason to believe that this trend will decline in the near future.

That is why it is crucial to follow a number of recommendations that may help prevent this type of attacks:

1. 1 Use up-to-date OS and application versions;
2. 2 Refrain from opening RDP access on the Internet unless necessary. Preferably, use VPN to secure remote access;
3. 3 Use modern endpoint security solutions, such as Kaspersky Endpoint Security for Business, that support behavior detection, automatic file rollback and a number of other technologies to protect from ransomware.
4. 4 Improve user education in the field of cybersecurity. Kaspersky Security Awareness offers computer-based training products that combine expertise in cybersecurity with best-practice educational techniques and technologies.

5. 5 Use a reliable data backup scheme.

Kaspersky products protect from this threat, detecting it as Trojan-Ransom.Win32.Wasted.d and PDM:Trojan.Win32.Generic. The relevant behavioral detection logic was added in 2017.

IoC

2cc4534b0dd0e1c8d5b89644274a10c1
