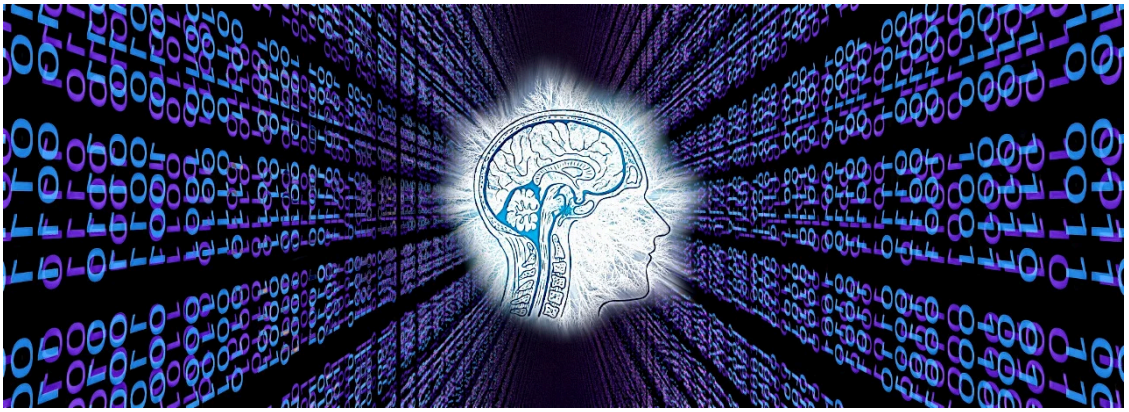
New Megacortex Ransomware Changes Windows Passwords, Threatens to Publish Data

By Lawrence Abrams

Published: 2019-11-05 · Archived: 2026-04-06 01:09:59 UTC

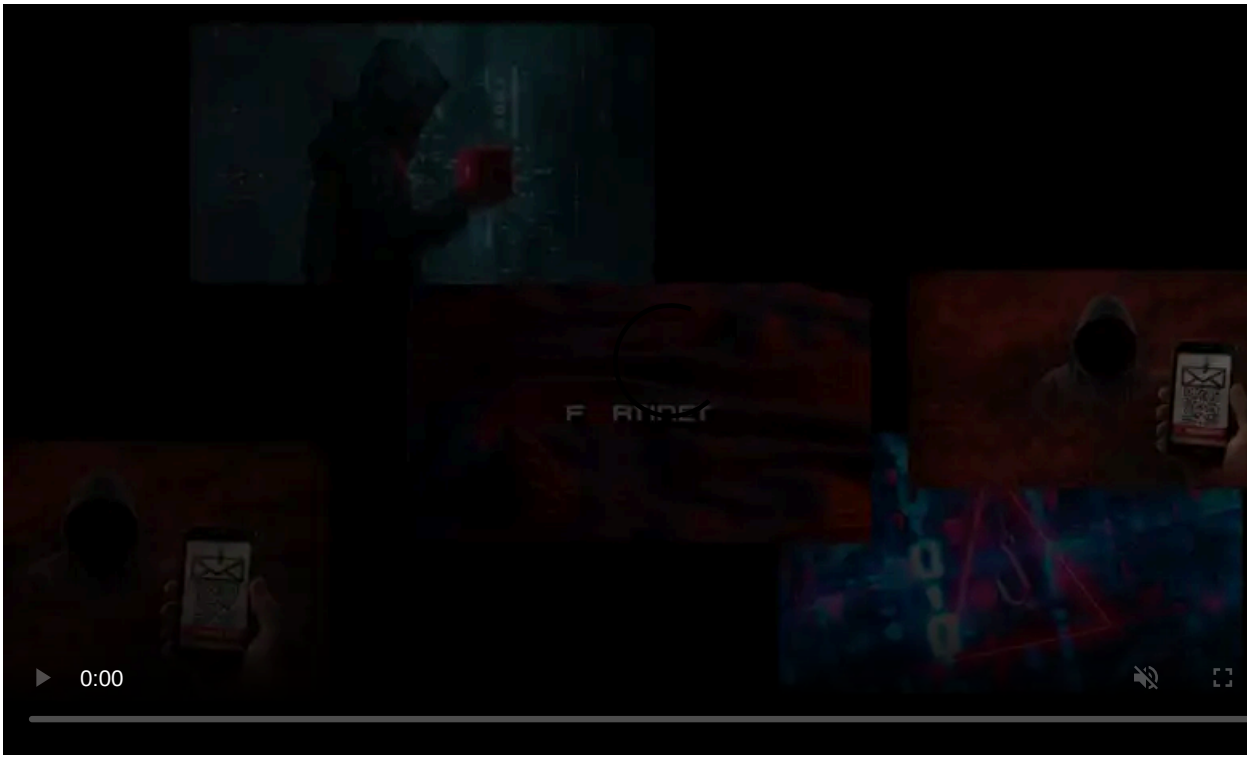


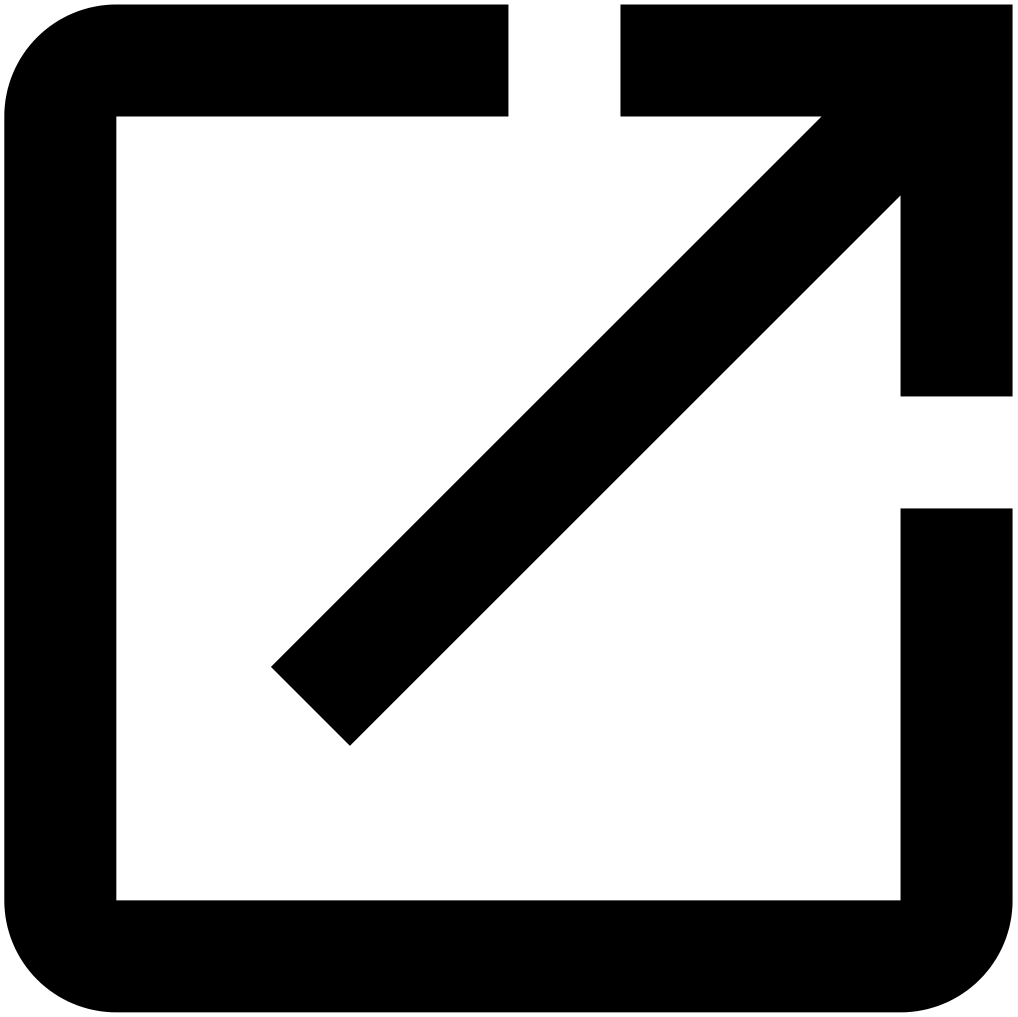
A new version of the MegaCortex Ransomware has been discovered that not only encrypts your files, but now changes the logged in user's password and threatens to publish the victim's files if they do not pay the ransom.

For those not familiar with MegaCortex, it is a targeted ransomware installed through network access provided by trojans such as Emotet. Once the MegaCortex actors gain access, they then push the ransomware out to machines on the network via an active directory controller or post-exploitation kits.

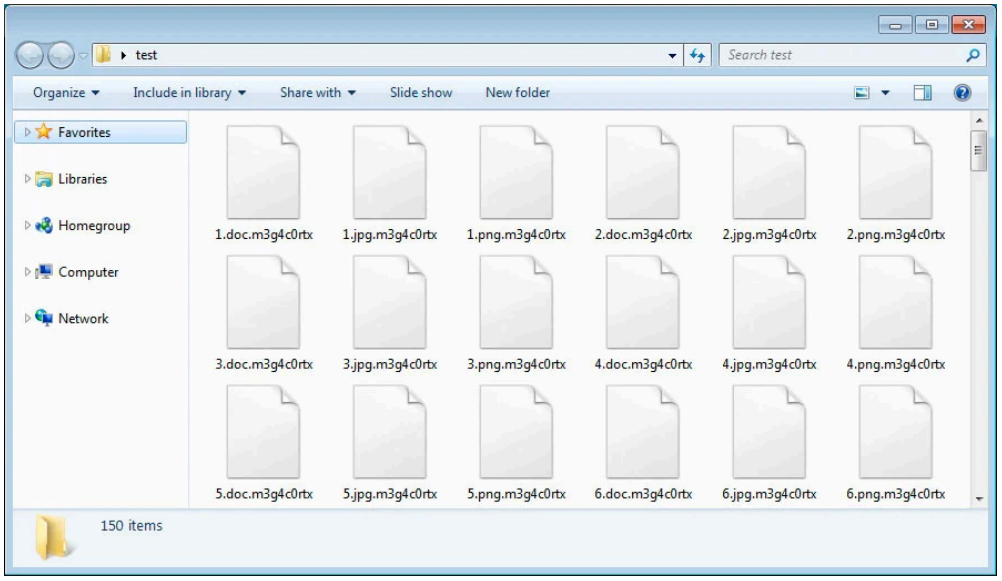
Significant changes in new MegaCortex version

In a new sample of the ransomware discovered by MalwareHunterTeam, reverse engineered by Vitali Kremez, and further analyzed by BleepingComputer, we see a new version of MegaCortex that has substantial changes from previous variants.


0:00

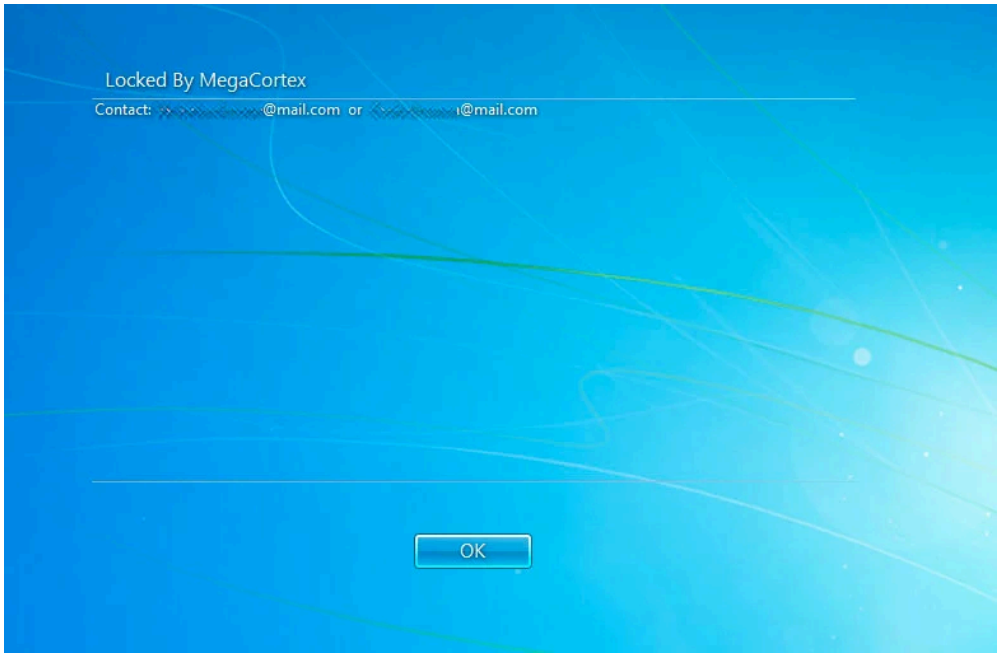


The most obvious change seen by victims is the new **.m3g4c0rtx** extension being used by the ransomware as shown below.



MegaCortex Encrypted Files

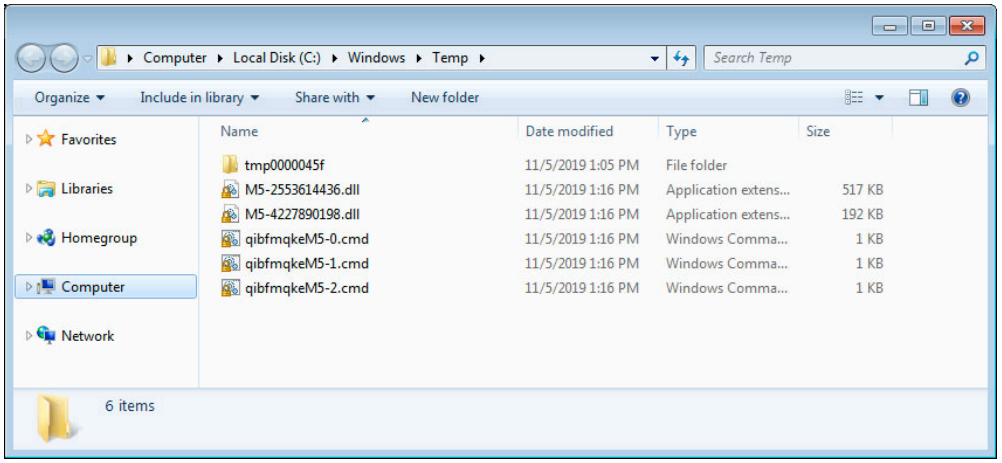
In addition, MegaCortex will now configure a legal notice on the encrypted machine so that it displays a basic "Locked by MegaCortex" ransom message with email contacts before a user even logs in.



MegaCortex Legal Notice

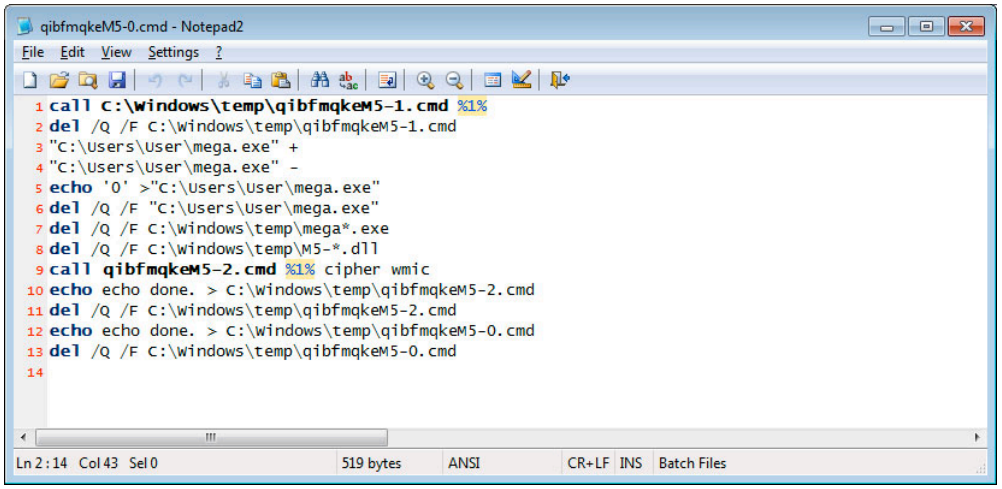
Behind the scenes, quite a bit has changed

When the main MegaCortex launcher is executed, it will extract two DLL files and three CMD scripts to C:\Windows\Temp. This launcher is currently signed with a Sectigo certificate for an Australia company named "MURSA PTY LTD".



C:\Windows\Temp Folder

These CMD files will execute a variety of commands that removes shadow volume copies, uses the Cipher command to wipe all free space on the C:\ drive, sets the Legal Notice, and then cleans up all the files used to encrypt the computer.

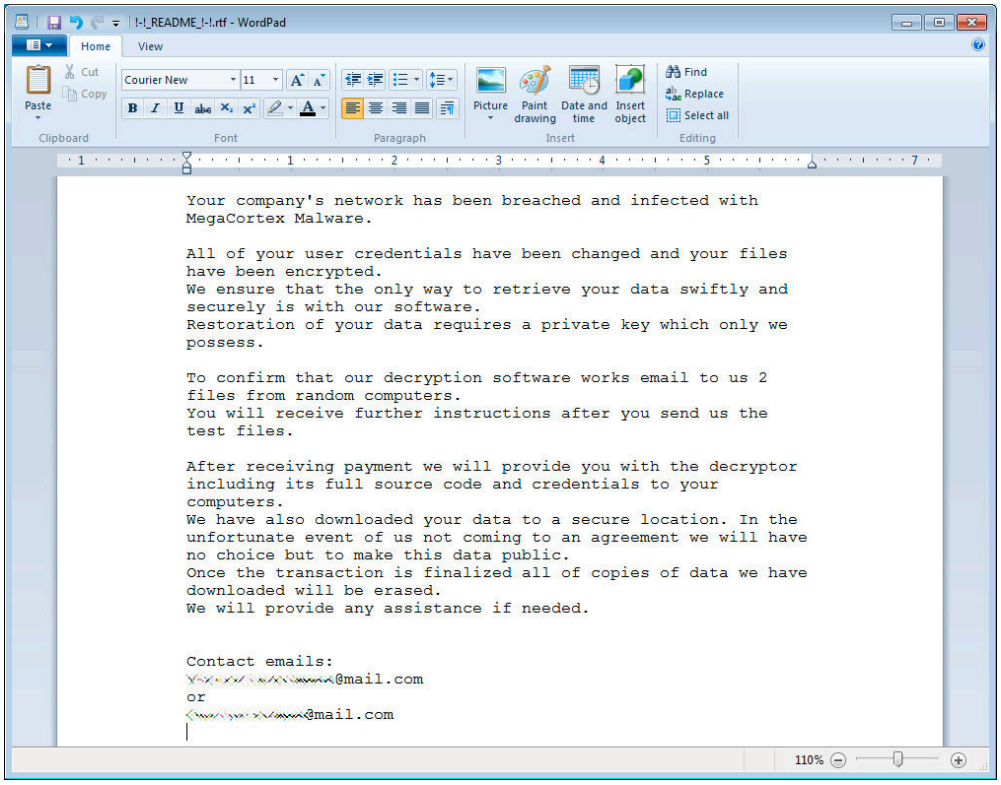


First CMD Script

Kremez told BleepingComputer in conversations that the two DLL files are used to encrypt the files on the computer. One DLL file is a file iterator that looks for file to encrypt and the other DLL will be used to encrypt the file.

These DLLs are not injected into any processes, but rather run via Rundll32.exe.

When done, victims will find a ransom note on the desktop titled **!-!_README_!-!.rtf** that contains some interesting comments that at first we dismissed as idle threats.



MegaCortex Ransom Note

After further analysis, we determined that at least one of the threats is true; the ransomware does indeed change the victim's password for their Windows account.

MegaCortex changes the victim's Windows password

It is not uncommon for ransomware developers to make threats that are not carried out in order to scare victims into paying.

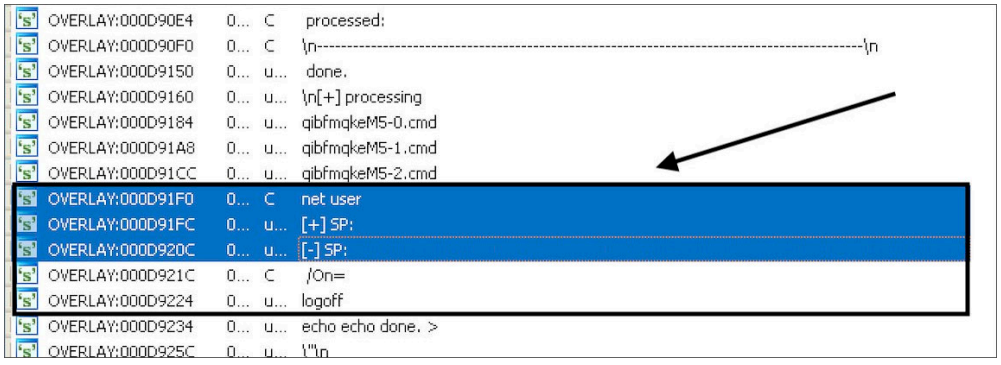
Due to this, when we saw that the ransom note stated that a victim's credentials have been changed, we dismissed it.

"All of your user credentials have been changed and your files have been encrypted."

After testing the ransomware and rebooting the encrypted computer, I discovered that I was unable to login to my account.

Further analysis of the code by Kremez confirmed that MegaCortex is indeed changing the password for the victim's Windows account.

It does this by executing the net user command when the ransomware is executed.



Net user command

This also explains why the attackers added a legal notice that is shown at the login prompt as the user will no longer be able to log in to access their desktop.

Threatens to publish victim's data

In addition to the proven claims of changing user credentials, the attackers have also changed the ransom note to state that victim's data has been copied to a secure location.

They then threaten to make this data public if a victim does not pay the ransom.

"We have also downloaded your data to a secure location. In the unfortunate event of us not coming to an agreement we will have no choice but to make this data public.
Once the transaction is finalized all of copies of data we have downloaded will be erased."

It is not confirmed if attackers have actually copied victims' files, but this threat should not be dismissed and victim's may want to confirm that the attackers actually have their files as stated when communicating with them.

If the MegaCortex actors are actually copying data, though, victims will now have to treat these attacks as a data breach going forward instead of just a ransomware infection.

This will ultimately add a whole new layer of complexity and risks to these types of attacks.

Update 11/7/19: Sectigo told BleepingComputer that they have revoked the certificate used by this malware on November 5th at 4:20 PM ET.

IOCs:

Hashes:

```
 ca0d1e770ca8b36f6945a707be7ff1588c3df2fd47031aa471792a1480b8dd53 [Launcher]
5ff14746232a1d17e44c7d095e2ec15ede4bd01f35ae72cc36c2596274327af9 [DLL]
e362d6217aff55572dc79158fae0ac729f52c1fc5356af4612890b9bd84fbcde [DLL]
```

Associated files:

```
 !-!_README_!-!.rtf
```

Ransom note text:

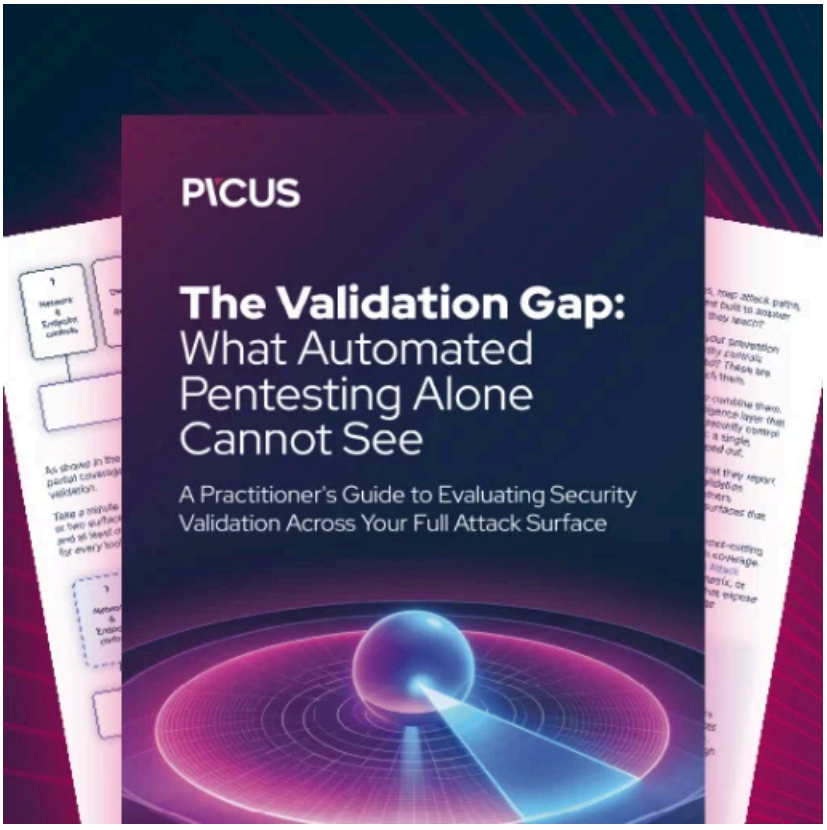
```
 Your company's network has been breached and infected with MegaCortex Malware.

All of your user credentials have been changed and your files have been encrypted.
We ensure that the only way to retrieve your data swiftly and securely is with our software.
Restoration of your data requires a private key which only we possess.

To confirm that our decryption software works email to us 2 files from random computers.
You will receive further instructions after you send us the test files.

After receiving payment we will provide you with the decryptor including its full source code and credentials to your comp
We have also downloaded your data to a secure location. In the unfortunate event of us not coming to an agreement we will
Once the transaction is finalized all of copies of data we have downloaded will be erased.
We will provide any assistance if needed.


Contact emails:
redacted@redacted.com
or
redacted@redacted.com
```



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-changes-windows-passwords-threatens-to-publish-data/