Marcus Murray (He/Him)

Founder of Truesec Group | Cyber Security Expert & Keynote Speaker | Protecting national interests and organizations against cyber threats | Threat Intelligence | Defense | Offence | Top 50 most influential in Tech 2022

Talks about #apt, #ransomware, #cyberattacks, #cyberdefence, and #cybersecurity

Stockholm, Stockholm County, Sweden · Contact info

9,029 followers · 500+ connections

VICTOR ZHORA

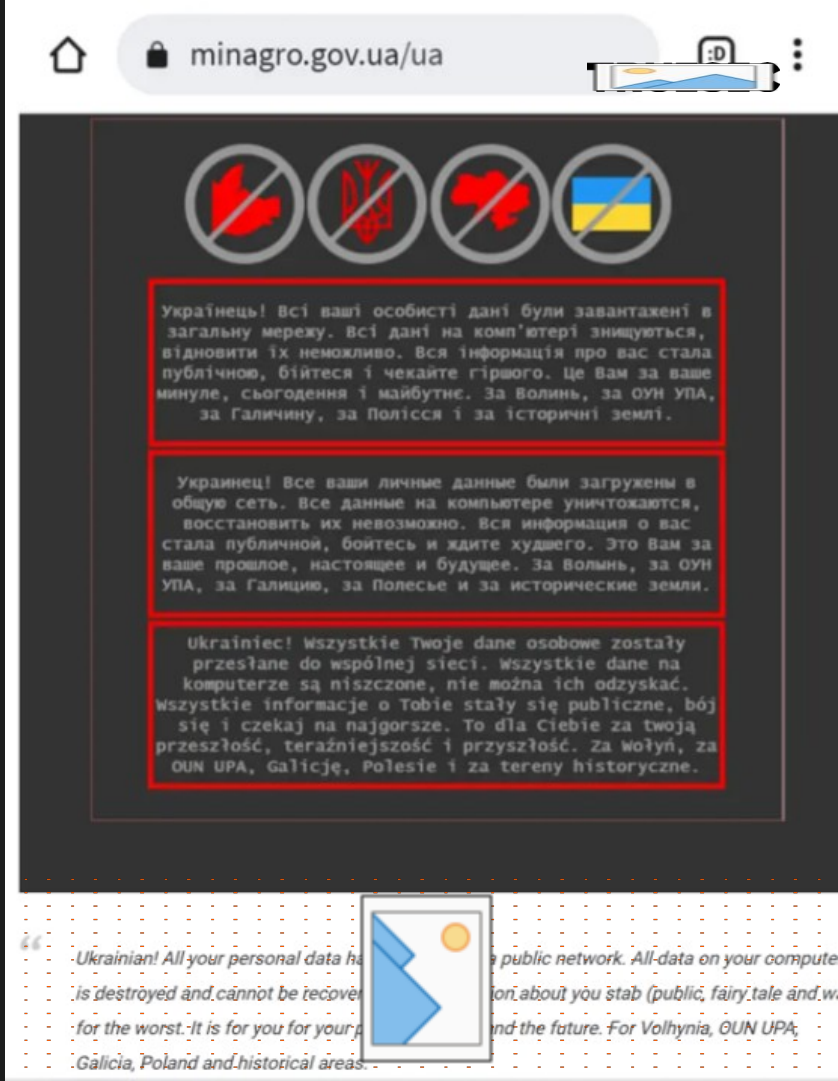
Top Ukraine cyber defense official visting Truesec


ESCALATION LADDER
WAR
Destroy and conquer
FEAR
Sense of hopelessness
DESINFORMATION
Change opinion

January 13 to 14: 70 Ukrainian government websites defaced!

- Ministry of Foreign Affairs
- Ministry of Education
- Etc.

- UND 1152, Belarus attributed



January 13-18: Wiperware attacks against Ukraine

- Victims span multiple government, non-profit, and information technology organizations.
- Destructive malware disguised as ransomware
- Attack initiated on January 13
- Announced on January 15
- WhisperGate

Experts Find Strategic Similarities b/w NotPetya and WhisperGate Attacks on Ukraine

January 22, 2022 Ravie Lakshmanan

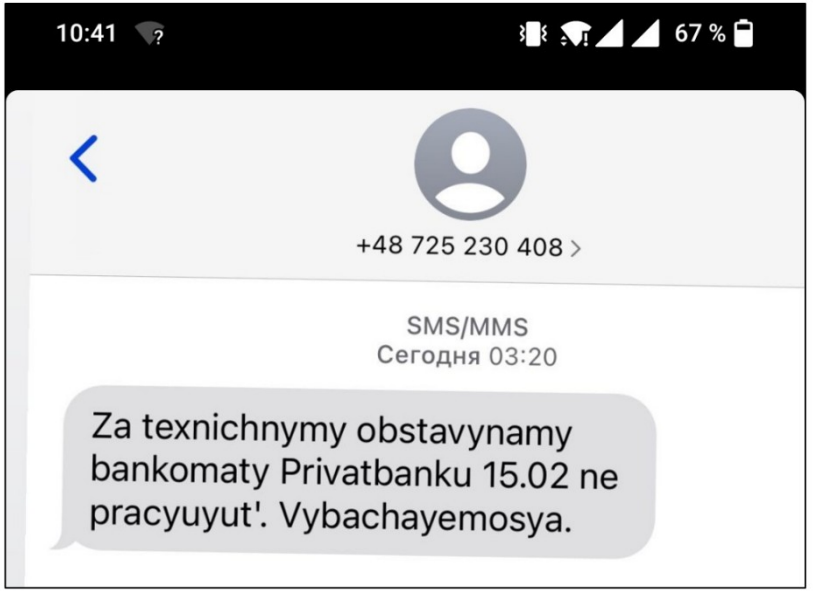
```
1 void __cdecl wipe_file(wchar_t *FileName)
2 {
3   size_t v1; // eax
4   wchar_t *new_filename; // esi
5   int v3; // edi
6   size_t v4; // eax
7   void *file_content; // [esp+28h] [ebp-20h]
8   FILE *Stream; // [esp+2Ch] [ebp-1Ch]
9
10  v1 = wcslen(FileName);
11  new_filename = (wchar_t *)malloc(2 * (v1 + 0x14));
12  v3 = rand();
13  v4 = wcslen(FileName);
14  swprintf(new_filename, (const size_t)"%", (const wchar_t *const)(v4 - 4), FileName, v3);
15  Stream = wfopen(FileName, L"wb");
16  file_content = malloc(1048576u);
17  memset(file_content, 0xCC, 1048576u);
18  fwrite(file_content, 1u, 1048576u, Stream);
19  fclose(Stream);
20  wrename(FileName, new_filename);
21  free(new_filename);
22  free(file_content);
23 }
```

Latest analysis into the wiper malware that targeted dozens of Ukrainian agencies earlier this month has revealed "strategic similarities" to NotPetya malware that was unleashed against the country's infrastructure and elsewhere in 2017.

The malware, dubbed WhisperGate, was discover oft last week, which said it observed the destructive cyber campaign targeting governi fit, and information technology entities in the nation, attributing the intrusions to threat cluster codenamed "DEV-0586."

February 15: Ukraine's defence ministry and banks hit by DDoS attack

- The Defense Ministry, the Foreign Ministry and two largest state banks etc unreachable.
- Bank customers reported problems with online payments, banking apps and, in very limited cases, accessing ATMs.
- These attacks were compounded with fraudulent SMS messages sent to Ukrainian phones in an attempt to create a panic.



Due to technical circumstances the bank 15.02 do not work sorry

February 23: Ukrainian banking and government websites hit by DDoS attack

- Ukrainian banks and government departments, including the Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs, Security Service (SBU) and Cabinet of Ministers became inaccessible following a large DDoS attack.

February 23: New form of destructive malware discovered in Ukrainian networks

- Hermetic wiper
- The wiper has been detected in Ukraine, Latvia and Lithuania.

- Ukrainian targets including financial organizations and government contractors

24 feb Attack on communication

- A cyberattack disrupted VIASAT broadband satellite internet access
- Ukraine military use Visasat for Command & Control

WASHINGTON, March 30 (Reuters) - Hackers who crippled tens of thousands of satellite modems in Ukraine and across Europe are still trying to hobble U.S. telecommunications company Viasat as it works to bring its users back online, a company official told Reuters.

Viasat Inc **(VSAT.O)** has been working to recover after a cyberattack remotely disabled satellite modems just as Russian forces pushed into Ukraine in the early hours of Feb. 24. The official said a parallel attack was launched at almost exactly the same time and used "high volumes of focused, malicious traffic" to try and overwhelm Viasat's network and was still ongoing.

Starlink terminals

Kyiv Mayor Vitali Klitschko and his brother, world boxing champion Wladimir Klitschko,


OFFICE
OF THE PRESIDENT
OF UKRAINE
ОФІС
ПРЕЗИДЕНТА
УКРАЇНИ

What if the war is lost in 1-3 days?

Anonymous
@YourAnonOne

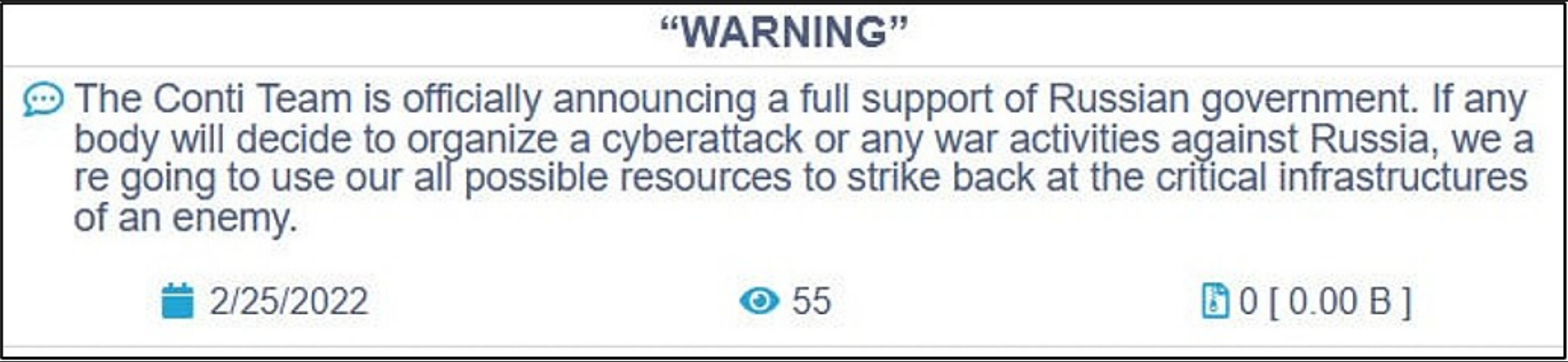
The Anonymous collective is officially in cyber war against the Russian government. #Anonymous #Ukraine

10:50 PM · Feb 24, 2022

316.9K Reply Share this Tweet

Read 9.3K replies

Feb 25:
Cybercriminals pick side



First war where the cyber component is fully integrated

- 1000+ Cyberattacks on Ukraine related to the war
- 15% sophisticated.
- DDOS / VIPERS
- Russia is exposing their capabilities
- Sets the standard for future conflicts.

Related risks for Northern European banking?

Articles

Invaders Preparing Mass Cyberattacks on Facilities of Critical Infrastructure of Ukraine and Its Allies

September 26, 2022

The kremlin is planning to carry out massive cyberattacks on the critical infrastructure facilities of Ukrainian enterprises and critical infrastructure institutions of Ukraine's allies. First of all, attacks will be aimed at enterprises of energy sector. The experience of cyberattacks on Ukraine's energy systems in 2015 and 2016 will be used when conducting operations.

By the cyberattacks, the enemy will try to increase the effect of missile strikes on electricity supply facilities, primarily in the eastern and southern regions of Ukraine. The occupying command is convinced that this will slow down the offensive operations of the Ukrainian Defence Forces.

The kremlin also intends to increase the intensity of DDoS attacks on the critical infrastructure of Ukraine's closest allies, primarily Poland and the

Would it be possible to deploy wipers in large banks?


Is ransomware still a threat?

Politics

Suspected Russian Ransomware Group Hacks Italian Energy Agency

- BlackCat gang says it stole 700 gigabytes in data from network
- Italy Premier Draghi, officials met Thursday to discuss hacks

By Daniele Lepido, Ryan Gallagher, and Alberto Brambilla
September 2, 2022 at 3:58 PM GMT+2

Listen to this article

▶ 3:26

Share this article

Follow the authors

@danielelepido

A hacker group with links to Russia has claimed responsibility for a recent ransomware attack targeting Italy's energy industry, amid an escalation the Rome-based government says could be related to the Russian invasion of Ukraine.

In a post published on the so-called dark web, the BlackCat group said it stole 700 gigabytes of data from networks controlled by Italy's GSE energy agency, and threatened to publish the information


Will Russia become a paria state?
Incorporates E-crime actors for profit

Putin orders FSB to go after western digital assets

As before, one of the priorities of the Foreign Intelligence Service is to assist in the industrial and technological development of our country, in strengthening its defense potential.

Conclusion:

The cyber threat keeps growing

Pragmatic solutions is key!

Marcus Murray (He/Him)

Founder of Truesec Group | Cyber Security Expert & Keynote Speaker | Protecting national interests and organizations against cyber threats | Threat Intelligence | Defense | Offence | Top 50 most influential in Tech 2022

Talks about #apt, #ransomware, #cyberattacks, #cyberdefence, and #cybersecurity

Stockholm, Stockholm County, Sweden · Contact info

9,029 followers · 500+ connections