

A Glimpse of the Future: Cyber Insecurity and Modern Conflict.

Martin LEE, Cisco Talos.

Active in Ukraine since 2016

Partnering with

- State Special Communications Service of Ukraine (SSSCIP)
- Cyberpolice Department of the National Police of Ukraine
- National Coordination Center for Cybersecurity (NCCC at the NSDC of Ukraine)

Assisting with

- Providing defensive guidance
- Assisting with forensic analysis
- Providing intelligence
- Assisting in hunting activities

Current Ukraine Cyber Assistance

Free offer of Cisco Security products
in Ukraine.

Dedicated threat hunting task unit.

660 people contributing to threat
detection.

“Our teams of threat hunters
have been around-the-clock
hunting in the data since the
invasion. They're stopping
attacks from happening.”

Future Conflict is...

Hybrid Threats

- Conflict in multiple domains
 - Disinformation & propaganda
 - Cyber disruption
- Cycle of abuse
 - Denial
 - Minimise
 - Blame victim

Disinformation Kill Chain

Recon

Find the cracks – Analyse target audience

Build

Weaponise – Prepare environment & personas

Seed

Launch Campaign – Design & deliver content

Copy

Fertilise – Share & duplicate content

Amplify

Watch Growth – Fake accounts, useful idiots

Control

Manipulate – Incite conflict, deny involvement


Effect

Harvest – Actions on objective

Proxy Agents

- Non-state actors
 - Act under state direction
 - Augment capability
- Provide
 - Plausible deniability
 - Action at arms length
 - Smoke screen for state actors

“WARNING”

 As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

2/25/2022


380

[READ MORE »](#)

Hacktivist Actors

Crowd sourcing offensive cyber capability

Susceptible to shifting narratives

Who chooses targets?

Varying levels of skill & engagement

Post-conflict deradicalization



Disruptive Cyber Attacks

- Wiper malware
 - Malicious software written to destroy systems and data
- Denial of service attacks
 - Prevent access to services
- Disruption of society
- Reduces ability to respond
- Promote disinformation

⚠ Behavioral Indicators

🔍 Artifact Flagged Malicious by Antivirus Service	95
🔍 Process Modified a File in a System Directory	85
🔍 VSSAdmin Service Autorun Disabled	85
🔍 Process Added a Service to the ControlSet Registry Key	72
🔍 A Service Was Set To Never Autorun Via The Registry	70
🔍 Process Requested Direct Access to Drive	66
🔍 A Registry Service Key Type Value Was Modified	50
🔍 Static Analysis Flagged Artifact As Anomalous	48
🔍 Process Uses Very Large Command-Line	32
🔍 Executable Signing Date Invalid	30
🔍 Executable Signed With Digital Certificate	10

Process Requested Direct Access to Drive

Score: 66 Hits: 99

Description

A process attempted to open a file handle using the direct device reference. This allows direct read and write from the device, without using the Windows drivers to process the filesystem. Legitimate programs may enumerate these drives to determine what resources should be presented to the user. Malicious programs may use this request enumerate system drives to identify further targets.

Information Stealers

- Malicious software
 - Conduct espionage
 - Steal credentials
 - Profile targets
 - Social engineering
 - Disinformation

⚠ Behavioral Indicators

🔍 A Document File Established Network Communications	81
🔍 VBA Macro May Call Shell	81
🔍 VBA Macro Has Action on Open	59
🔍 Office Document Contains a VBA Macro	56
🔍 Outbound HTTP GET Request	56
🔍 Static Analysis Flagged Artifact As Anomalous	48
🔍 File Downloaded to Disk	27
🔍 Sample Communicates With Only Benign Domains	19
🔍 DNS Response Contains Low Time to Live (TTL) Value	7

Infrastructure as a Target

Disrupt critical national infrastructure
Disrupt communications

April 12, 2022
3:32 PM GMT+1
Last Updated a month ago

Europe

Ukraine says it thwarted Russian cyberattack on electricity grid

By James Pearson

2 minute read

[Twitter](#) [Facebook](#) [LinkedIn](#) [Share](#) [Email](#) [Bookmark](#)



Building Resilient Societies

Prepare

Awareness



- Threat actors will target you (even if you think that you are insignificant)
- Disinformation campaigns
- Denial of service attacks
- Defacement of website
- Wiper malware
- Supply chain attacks

Media Literacy



- Identify disinformation

Prepare

Prevention



- Identify & manage risks
- Aggressively harden systems

Detection



- Protection everywhere
- Visibility & vigilance
- Proactive threat hunting

Response



- Plan in advance
- Redundant systems & fail over
- Test & rehearse

Stay Connected and Up To Date

Spreading security news, updates, and other information to the public.



Talos publicly shares security information through numerous channels to help make the internet safer for everyone.

Thank
you!

TALOSINTELLIGENCE.COM



blog.talosintelligence.com



[@talossecurty](https://twitter.com/talossecurty)



TALOS™

TALOSINTELLIGENCE.COM