MANDIANT®

The Threat Is Stronger Than The Execution

Realities of Hacktivism in the 2020s

Blake Djavaherian

Senior Analyst, Mandiant

About The Author

- Formerly: CrowdStrike
  - Focus on State-Nexus and Hacktivist Activity
- Currently: Mandiant
  - Mandoogle?
- Previously Spoken On:
  - Threat Intelligence Investigations
  - Attribution

WHO CARES?

Ease of access to offensive cyber capabilities—combined with both long-term and acute geopolitical developments—increasingly enables the formation of comparatively sophisticated, professionalized hacktivist organizations able to produce genuine impacts against target entities.

(Typical) Hacktivist Group Characteristics

Skids, Kids, and Scripts

Loose Group Structures

- Individualistic
- Egotistical
- Informal and Sporadic

Lacking Technical Capabilities

- Reliance on open-source tools
- Rapid, shallow incorporation of tooling
- Little support for skills development

Pervasive Immaturity

- Inconsistent bouts of activity
- Lacking (or purposefully disregarded) OPSEC
- Incohesive vision

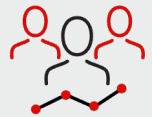
Resulting In:

Collectives

- Comprised of loosely affiliated individuals
- Broad ideological belonging
- Swarm-like

Working Groups

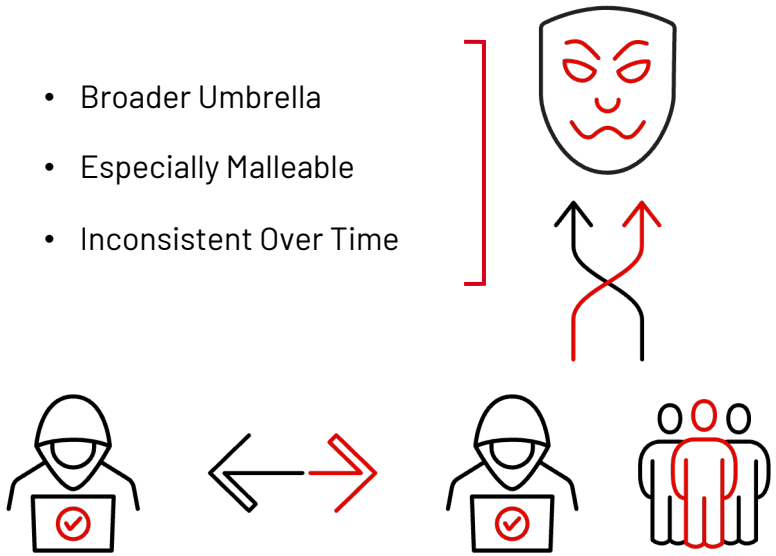
- Greater cohesion, singular primary identity
- Often form around cultural commonalities
- Interact with one another within ecosystems



Hacktivist Group Characteristics (cont.)

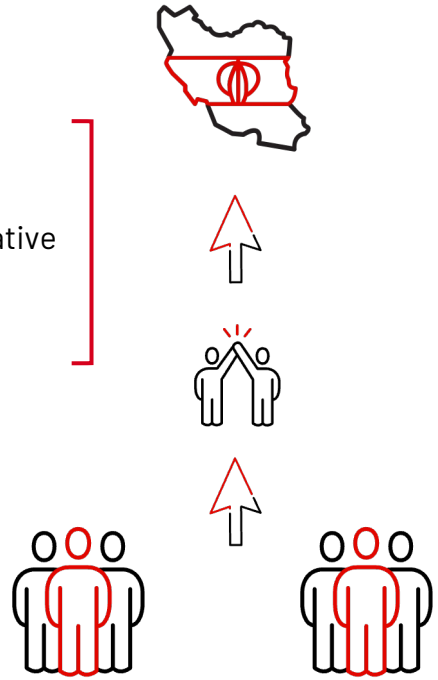
Collectives:

- Broader Umbrella
- Especially Malleable
- Inconsistent Over Time



Working Groups:

- Purpose Over Person
- Somewhat More Collaborative
- Culturally Tempered



(Typical) Capabilities

Denials, Defacements, and Data Leaks, Oh My!

Denials of Service

- Rapid capability uptake
- Fleeting effects

Defacements

- Similarly transient impacts
- Effective for attracting immediate attention

Data Leaks

- Parallels with more conventional cyber intrusions
- Significantly more difficult to implement
- Often falsely claimed

RANSOMWARE

Threat actors aiming to cause disruption purely for the sake of it—including hacktivist groups—are increasingly turning to ransomware as a method to achieve their goals.

The Belarusian Cyber Partisans

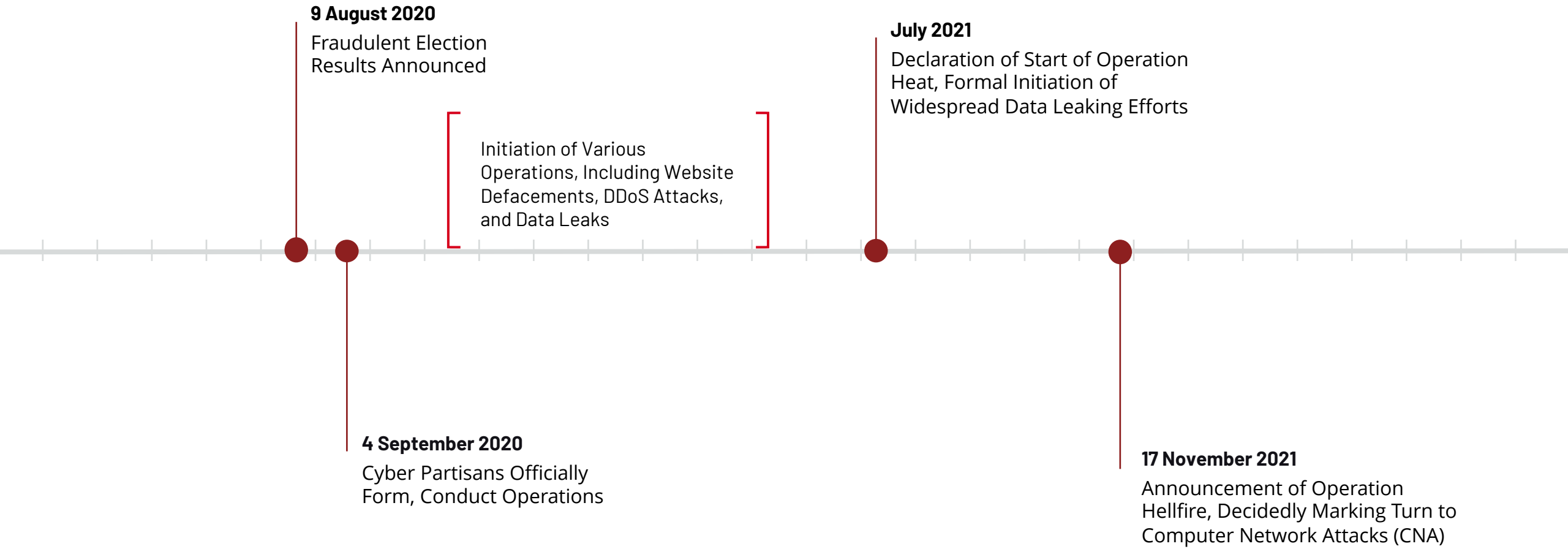
Formation, Rise to Prominence, and Ongoing Evolution

Protests in Belarus

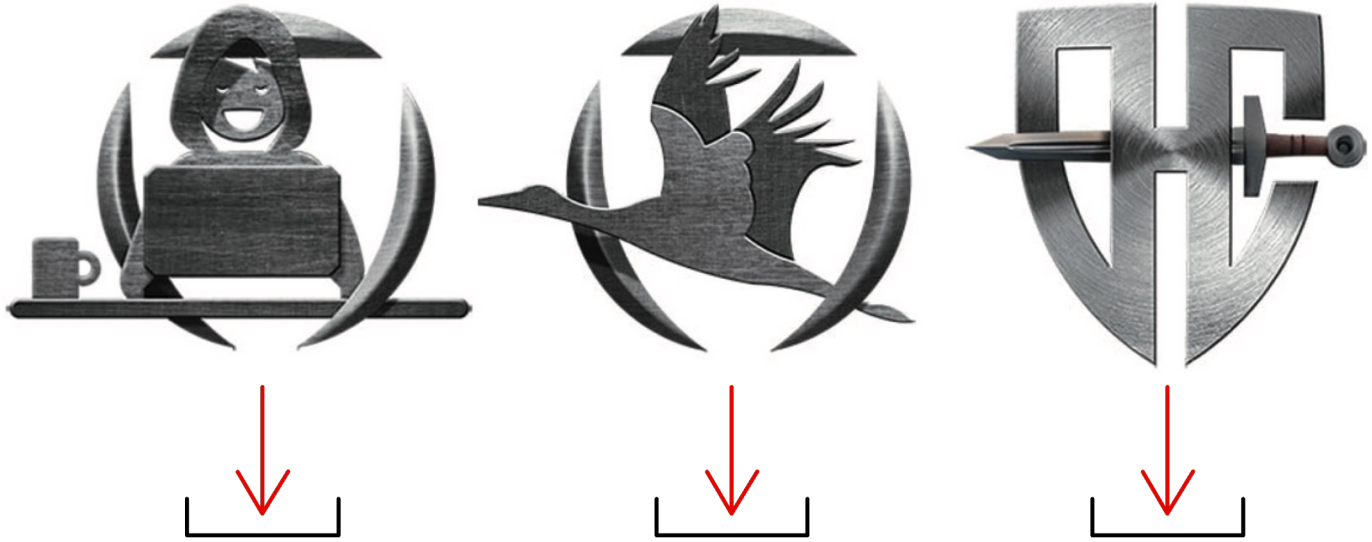
- Response to Fraudulent 2020 Presidential Elections
  - Public Economic, Pandemic, & Systemic Woes
- Subsequent Brutal Government Suppression
  - Crackdown on Journalists and Protesters
  - Large-Scale Deployment of Domestic Security Forces
  - Western Condemnation, Economic Sanctions Largely Ignored
- Protests Endure into 2021
  - Prominent Role of Technology for Communication, Coordination, and Collective Security

Timeline of Cyber Partisans Activity

Minsky Business



Collaborations



Cyber Partisans
Cyber Expertise to Enable Digital Espionage and Sabotage Operations

Flying Storks
Physical Sabotage Against Belarusian Infrastructure and Government Entities

PSS
Training and Education to Assist Protestors During Mass Mobilizations

Bonus Collaborations:

ByPol, Journalistic Outlets, the Public (via an External Spokesperson)

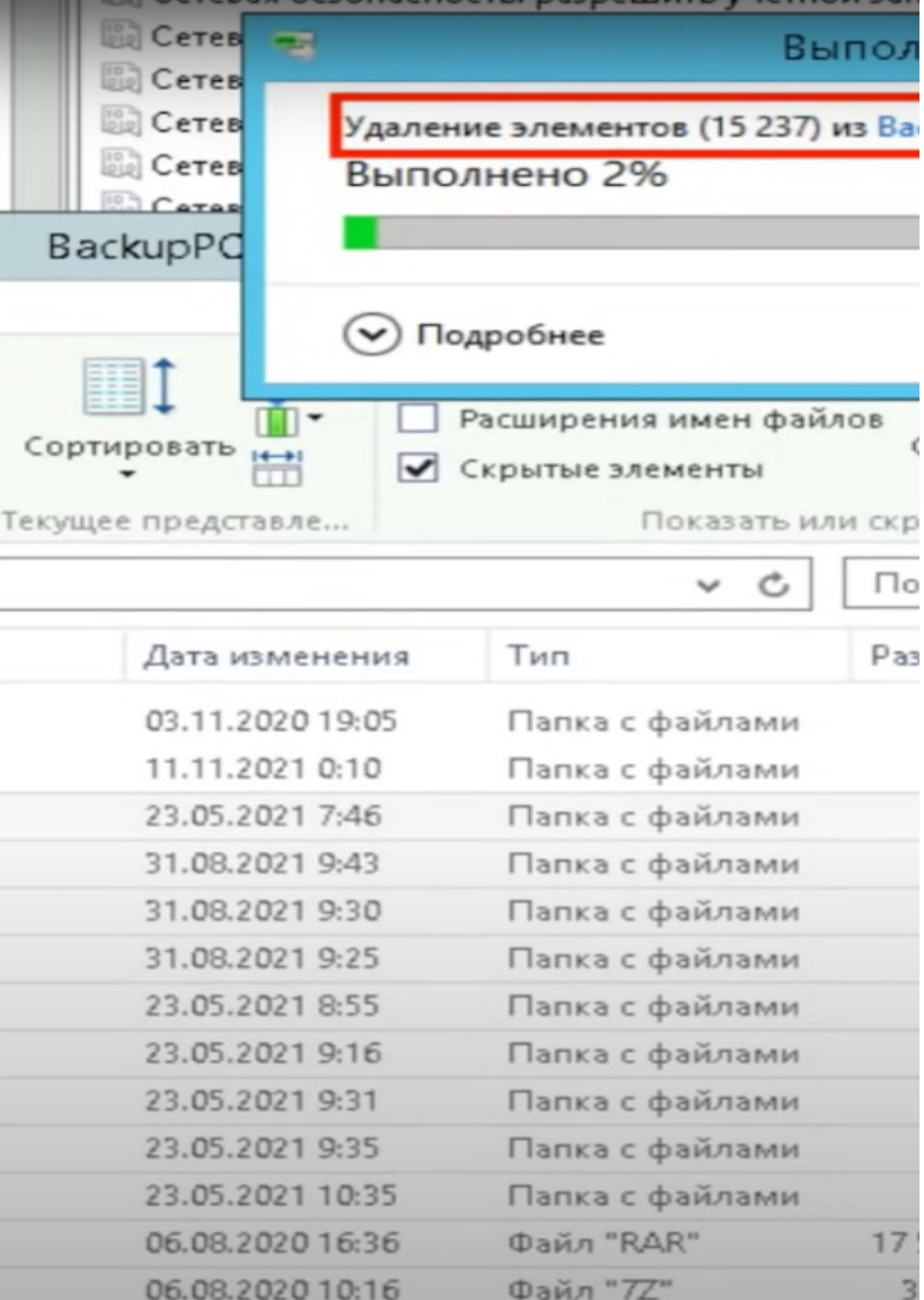
Each Member Group Party to the Suprativ Alliance...

–

- The Cyber Partisans
- Flying Storks
- People's Self-Defence Squads

–

...Performs a Specific Function Related to the Common Goal of Identifying, Publicizing, and Disrupting the Activities of the Lukashenko Government, with the Overall Intention of Regime Change.



TRADECRAFT

- 25 January 2022: Leaked Incident Response Write-Up Provides Clarity Toward Certain Cyber Partisans TTPs
  - Living-Off-The-Land Tactics
  - Deployment of Open-Source Tools
  - Ransomware/Wiper Tools?

Summary of Attack:

- Initial access via BlueKeep RCE (CVE-2019-0708) in RDP in a Windows Server 2008 R2 system
- Used the 3proxy[.]ru service to launch attacks from a VPS
- Use of Mimikatz to dump LSASS (SYSTEM level privileges are required however, how they obtained these is currently unclear)
- Nmap to identify systems (used Nmap to identify systems with Port 3389 open)
- Used RDP to move laterally
- Eventually landed on the victim's Domain Controller
- Configured TCP port forwarding to open Port 3389 to the internet for persistent access
- Deleted data (such as employee records) from live and backup systems

Figure: Summary of Operation Detailed in Leaked IR Report (Credit: Curated Intel)

War in Eastern Europe

- Russian Invasion:
  - 24 February 2022
- Consistent Belarusian Government Complicity
  - Logistical Support for the Russian War Effort
  - Threatened Expansions to Participation in the Conflict
- Immediate, Strong Response by Various Hacktivist Groups
  - Competition Amongst and Between One Another

Actions Amidst Conflict in Ukraine

Belarusian Cyber-Partisans
@cpartisans

At the command of the terrorist Lukashenka, #Belarusian Railway allows the occupying troops to enter our land. We encrypted some of BR's servers, databases and workstations to disrupt its operations. ❗ Automation and security systems were NOT affected to avoid emergency situations

6:08 AM · Jan 24, 2022 · TweetDeck

Cyber Response

- Continued Focus on Belarus-Owned Infrastructure
- Purposefully Avoid Direct Targeting of Russian Infrastructure with Disruptive Capabilities
- Data Leaks Implicating Russian Malfeasance, Incompetence, or Connections to Belarusian Officials
- Open Social Media Support For Ukraine

Unknowns

Donald Rumsfeld, Could You Please Stand Up

- Particulars Surrounding Group Structure
  - Bases of Operation, Nationalities Represented, or Hierarchy
  - Individual Roles, Backgrounds, and Divisions of Manpower
- Custom Tool/Capability Development
  - Preparations for a So-Called "Day X"
  - Alleged Development of Undisclosed Custom Tools (X-App")
- Extent of Persistence
  - Likely Sustained Access to Multiple Belarusian Entities

While the Cyber Partisans have not revealed the full range or planned development of their tooling, information available via open sources and through group disclosures indicates their technical capabilities—including those meant to enable data exfiltration, targeted encryption, or both—continue to grow and evolve.

OUTLOOK

While hacktivists continue to rarely form effective, lasting group structures, the rise, demonstrated impact, and ongoing evolution of Belarus's Cyber Partisans suggests the formation of such professionalized entities is not only increasingly possible, but a reality, in times of regionally concentrated strife.

MANDIANT®

YOUR CYBERSECURITY ADVANTAGE

Thank You