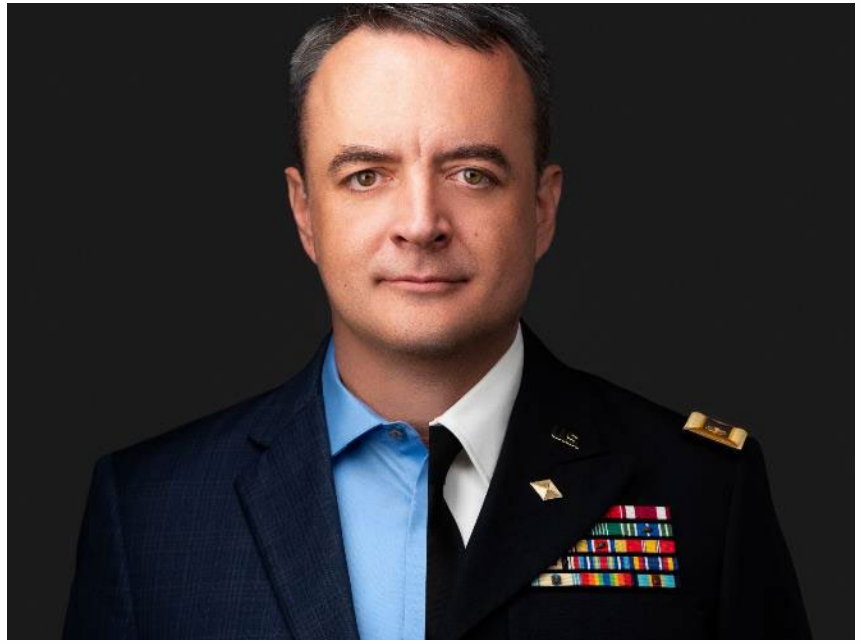
Beers, Bitcoins & Feds

Evolution of Russian cyber/hybrid warfare & its' impacts on the cybercriminal landscape

Evgueni Erchov

Head of Security Research & Strategy
October 17th, 2024

Introductions



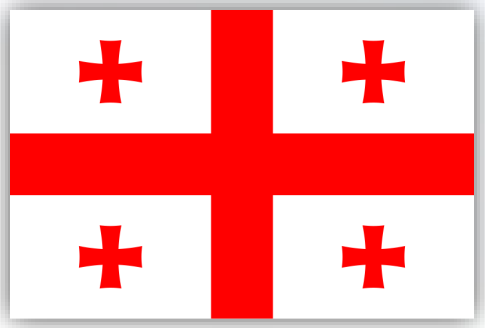
Head of Security Research & Strategy
AreteIR
EErchov@areteir.com

Information Systems Engineer / Cyber Ops
USAR, 78th TD
Evgueni.A.Erchov.mil@army.mil

2007 Estonia

- Misinformation campaigns
- Web site defacements
- FSB-organized crowdsourcing of hacktivists
- DDoS attacks on government, media and critical infrastructure organizations

2008 Georgia



- Misinformation campaigns
- Web site defacements
- FSB-organized crowdsourcing of hacktivists
- DDoS attacks on government, media and critical infrastructure organizations
- **BGP-highjacks (through SORM?)**
- **Kinetic attack of comms facilities**

SORM – «COPM»

Stands for “System for Operative Investigative Activities”
Note: All LE & IC agencies have access to it

- SORM-1: Phone calls & metadata interception
- SORM-2: Internet communications interception
- SORM-3: All communications interception & preservation

All Russian telecom providers are required to install SORM equipment.

2014 Crimea annexation

- Misinformation campaigns
- Web site defacements
- FSB-organized crowdsourcing of hacktivists
- DDoS attacks on government, media and critical infrastructure organizations
- **Covert unit attack of Ukrtelecom facilities**
- **Electronic Warfare deployment (***incl satcom jammers)*

Note: SORM-3 was fully deployed in the area and special forces units were pre-positioned to provide "security for Sochi Olympic games"

Odd “Olympic” Timing

Date	Olympics	Conflict
Aug 2008	Beijing, China	Georgia
Feb 2014	Sochi, Russia	Crimea annexation
Feb 2022	Beijing, China	Ukraine

Ukraine/Russia Conflict Update

Background

- After the start of invasion in Feb-2022 several state-sponsored, cyber criminal and hacktivist groups joined the conflict
- Relocations:
  - 12m+ citizens left Ukraine since Feb-2022
  - 5m+ males under 55yo fled Russia after mobilization announcement in Sep-2022
- Significant events so far:
  - Data wiper malware deployments
  - Email compromises
  - Misinformation campaigns (including Deepfakes)
  - DDoS
  - Web site defacements
  - Exfiltration/leak of data
  - Compromise of a ViaSat satellites and Starlink terminals

Outlook

- Russia may leverage state-sponsored APT against organizations in US/EU/UK
- APTs that were involved in previous conflicts:
  - APT 28
  - APT 29
  - Turla
- Industries at risk:
  - Government / Military organizations
  - Energy / Critical infrastructure
  - Financial
  - Non-profits / Think tanks

Criminal Landscape Changes
Top Drivers

Ukraine/Russia War

~8mln citizens of Ukraine left country
~5mln males under 55yo left Russia to avoid mobilization

Successful Law Enforcement Operations

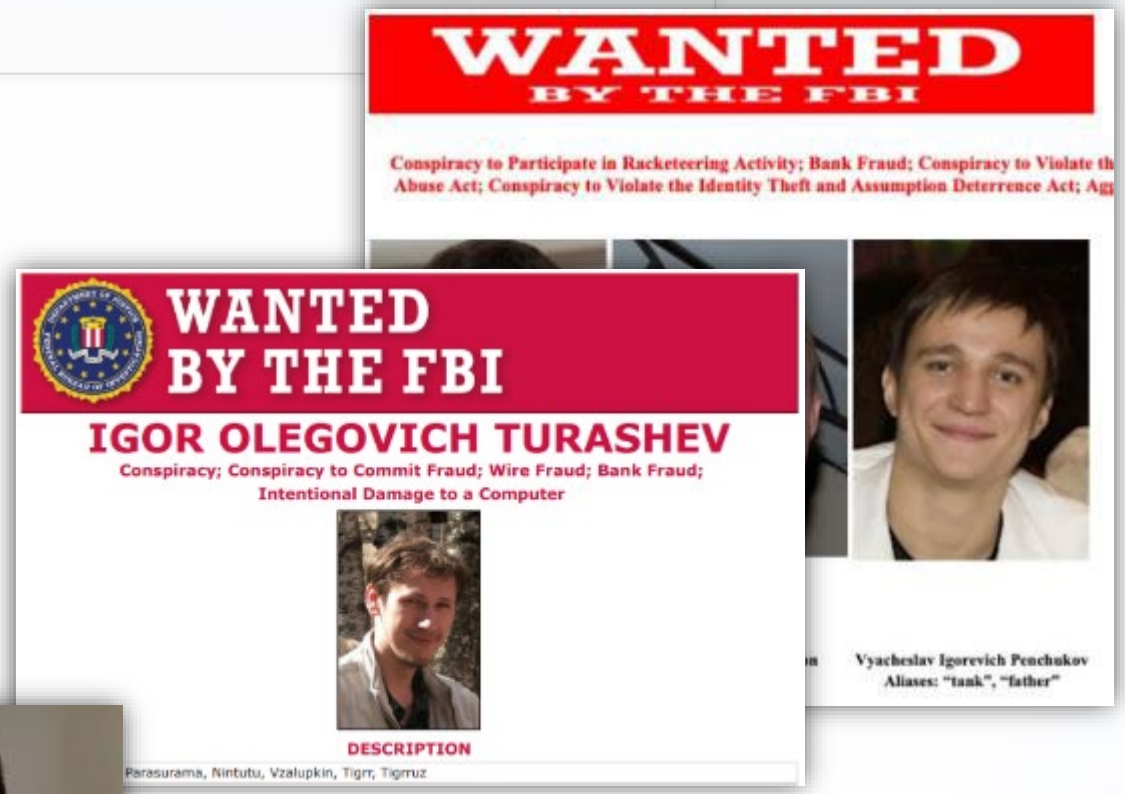
Top Criminal groups are being successfully targeted by International Law Enforcement (LE) operations

1st Known Arrest – Racoon RaaS

- Mark Sokolovsky (an alleged developer and operator of Racoon InfoStealer RaaS):
  - Left Ukraine around March 4th, 2022
  - Arrested in Netherlands on March 20th, 2022
  - Being extradited to the USA

“And the Beat Goes On”

- **Vyacheslav “tank” Penchukov**
  - Suspected JabberZeus day-to-day manager
  - Indicted & sanctioned by US Gov in 2014
  - Arrested in Geneva, Switzerland in Nov-2022
- **Anatoly Legkodymov**
  - Suspected operator of Bitzlato illegal Crypto exchange
  - Arrested in Miami, FL in Jan-2023
- **Igor Turashev**
  - Suspected “Evil Corp” 2nd in-command
  - Indicted & sanctioned by US Gov in 2019
  - Arrested in Germany in Mar-2023



Top Takedowns 2023 & 2024: “Citius, Altius, Fortius”

- Jan-2023 – Hive
- Oct-2023 – Ragnar Locker
- Dec-2023 – Black Cat / ALPHV
- Feb-2024 – Lockbit
- May-2024 – Operation Endgame

Market Share

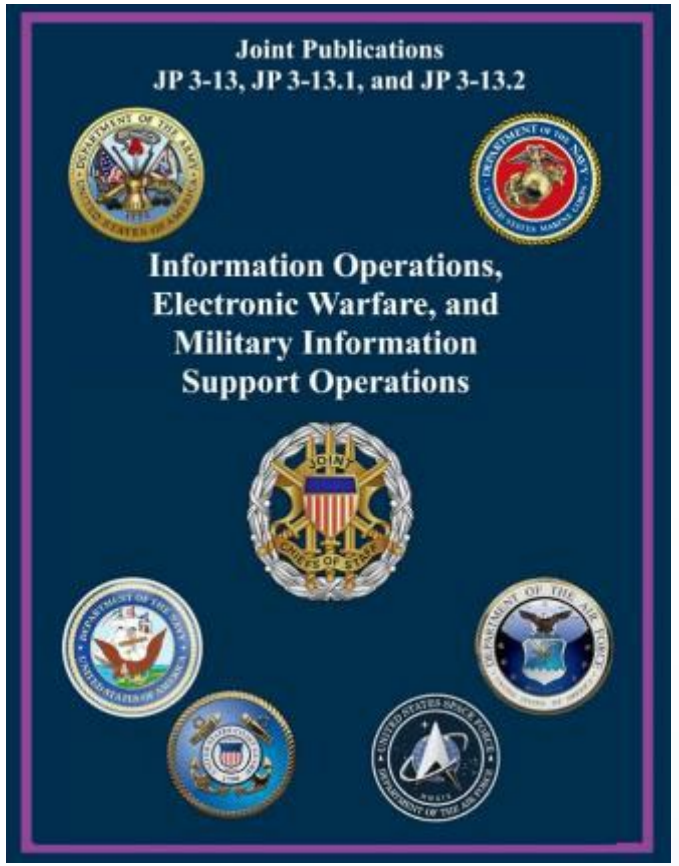
Period	# of Named TAs	# of Unidentified TAs
Q1 2024	49	27
Q1 2023	57	21

Period	Share	Top 3 Groups
Q2 2024	27.6%	Akira / LockBit / Medusa
Q1 2024	32.7%	LockBit / Akira / BlackSuit
Q2 2023	37.7%	ALPHV-BlackCat / LockBit / Akira
Q1 2023	35.1%	LockBit / ALPHV-BlackCat / Black Basta

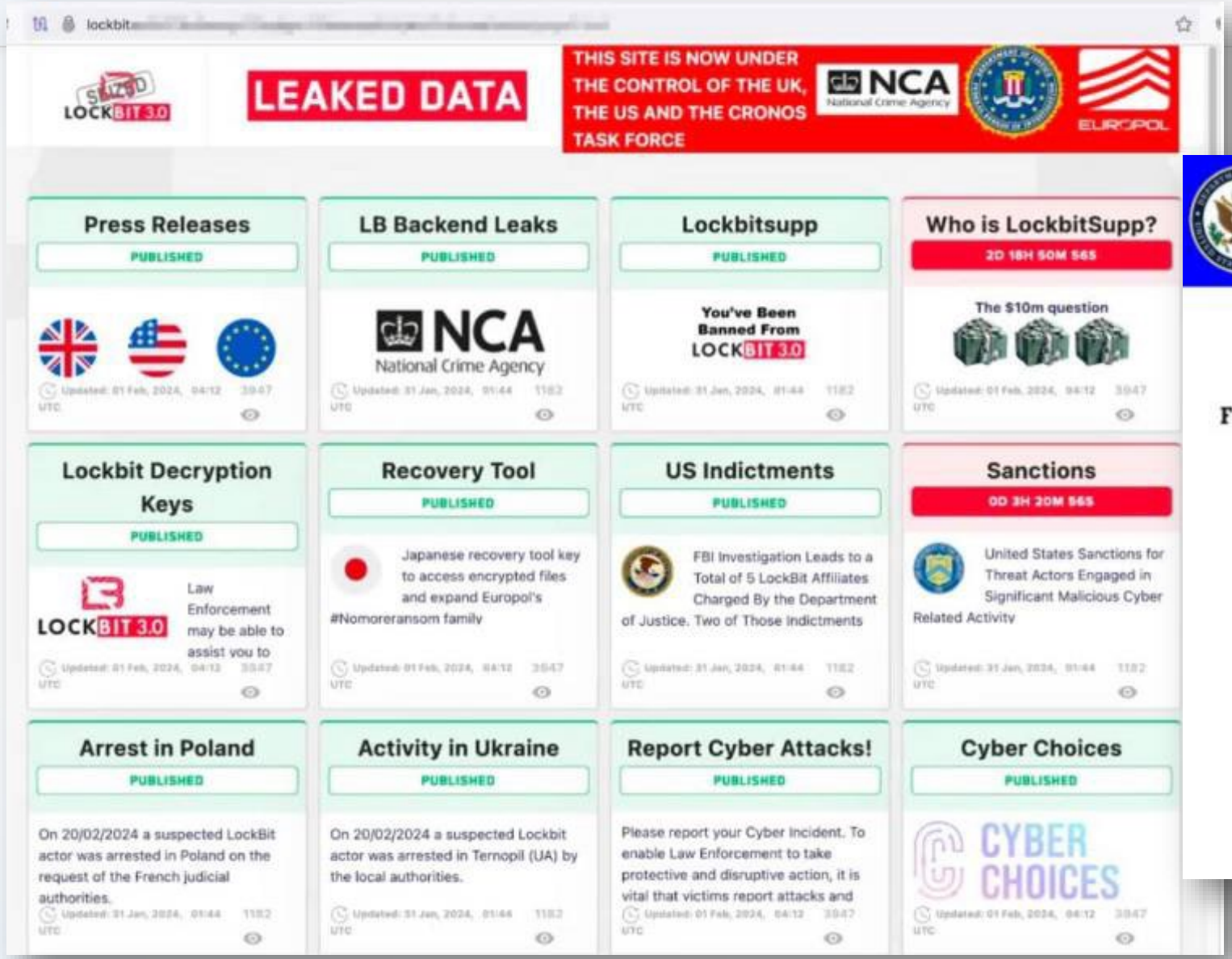
LE Information Operations (IO)

IO tactics in asymmetric warfare:

- Influencing public opinion
- Psychological operations
- Cyberwarfare
- Counterintelligence
- Strategic communications

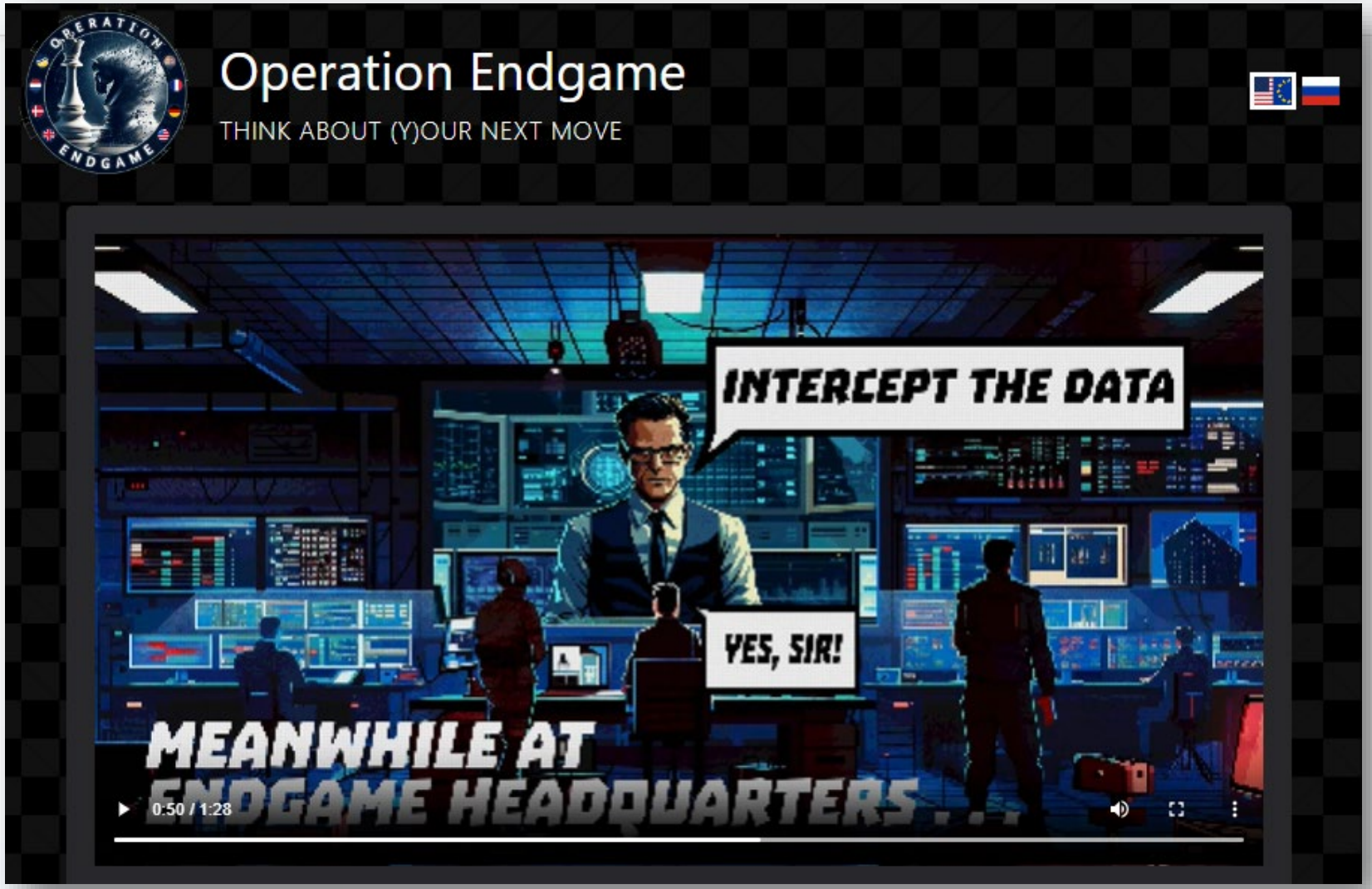


LockBit


LEAKED DATA
THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE
NCA
National Crime Agency
EUROPOL
Press Releases
PUBLISHED
LB Backend Leaks
PUBLISHED
NCA
National Crime Agency
Lockbitsupp
PUBLISHED
You've Been Banned From LOCKBIT 3.0
Who is LockbitSupp?
2D 18H 50M 56S
The $10m question
Lockbit Decryption Keys
PUBLISHED
LOCKBIT 3.0
Law Enforcement may be able to assist you to
Recovery Tool
PUBLISHED
Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family
US Indictments
PUBLISHED
FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments
Sanctions
0D 3H 20M 56S
United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity
Arrest in Poland
PUBLISHED
On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French judicial authorities.
Activity in Ukraine
PUBLISHED
On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.
Report Cyber Attacks!
PUBLISHED
Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and
Cyber Choices
PUBLISHED
CYBER CHOICES


REWARD
OF UP TO
$10,000,000 USD
FOR INFORMATION LEADING TO THE ARREST AND/OR CONVICTION OF LOCKBIT RANSOMWARE VARIANT ADMINISTRATOR
DMITRY YURYEVICH KHOROSHEV

Operation Endgame



Operation-Endgame[.]com

Ransom Demands & Payments: 2023 & 2024 YTD

	H1 2023	H2 2023	H1 2024
% of Time a Ransom Paid	34.4%	32.2%	26.5%
Median Demand	$525k	$476k	$450k
Median Payment	$155k	$140k	$145k

Artificial Intelligence

- Phishing emails
- Deepfakes
- Malware development

 |

Future Predictions

- TAs' groups will continue to split/re-brand
  - Increased importance of:
    - Dark Web Search & Monitoring
    - Reverse Engineering
    - Cyber Threat Intel
    - Forensics
    - Blockchain analysis
- New platforms will be targeted (e.g. MacOS & mainframes)
- Ukraine / Russia war increases risk for:
  - Government / Military organizations
  - Energy / Critical infrastructure
  - Financial
  - Non-profits / Think tanks

Q&As

Head of Security Research & Strategy
AreteIR
EErchov@areteir.com

Information Systems Engineer / Cyber Ops
USAR, 78th TD
Evgueni.A.Erchov.mil@army.mil

Disclaimer

Information contained within this presentation is business confidential and proprietary to Arete Advisors, LLC and provided for educational purposes only. This information should not be considered as legal advice.

Do not duplicate or distribute without written permission from Arete Advisors, LLC.