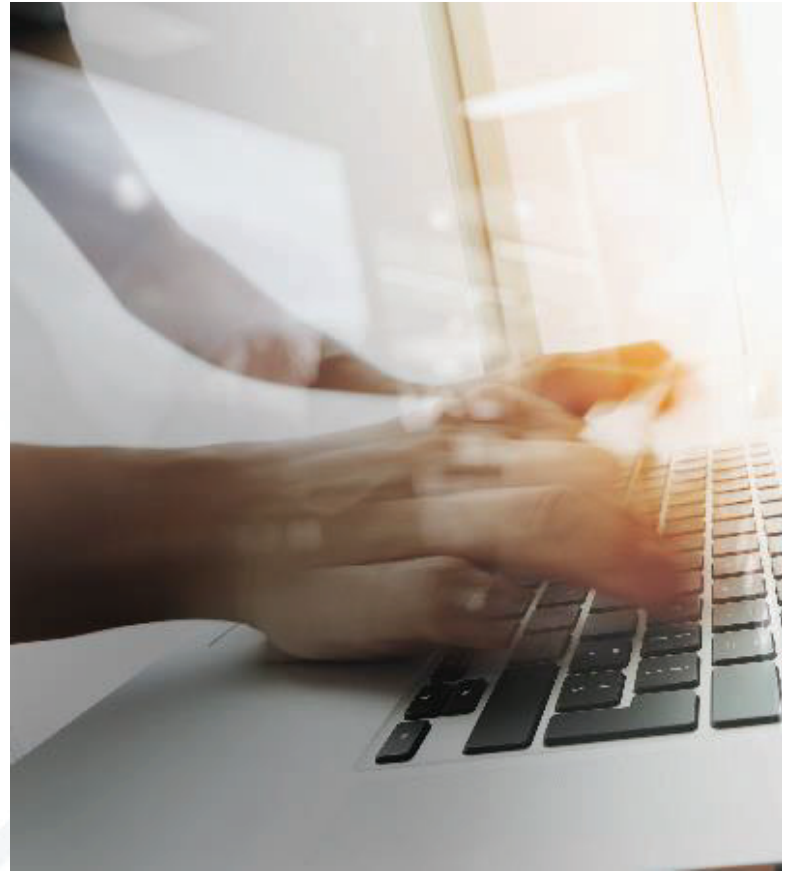




# CYBER TRENDS FROM THE WAR IN UKRAINE

Augusto Morales, PhD  
Technology Lead, Threat Solutions | Office of CTO  
Check Point Software Technologies  
IEEE Senior Member



## Agenda

- Current cyber attack trends in Ukraine
  - Tactics and techniques used
  - Lives examples
- Security practices to secure your workforce
- Q/A

# Check Point: The Largest Global Cyber Security Company

-  Global Leader – 100,000+ Customers, 88+ Countries, 6,200+ Partners
-  Over 25 years of cutting edge technologies, Industry's most visionary player
-  Innovation leadership – highest number of developers
-  Traded on Nasdaq since 1996 - CHKP
-  5,300+ Employees worldwide, top talent

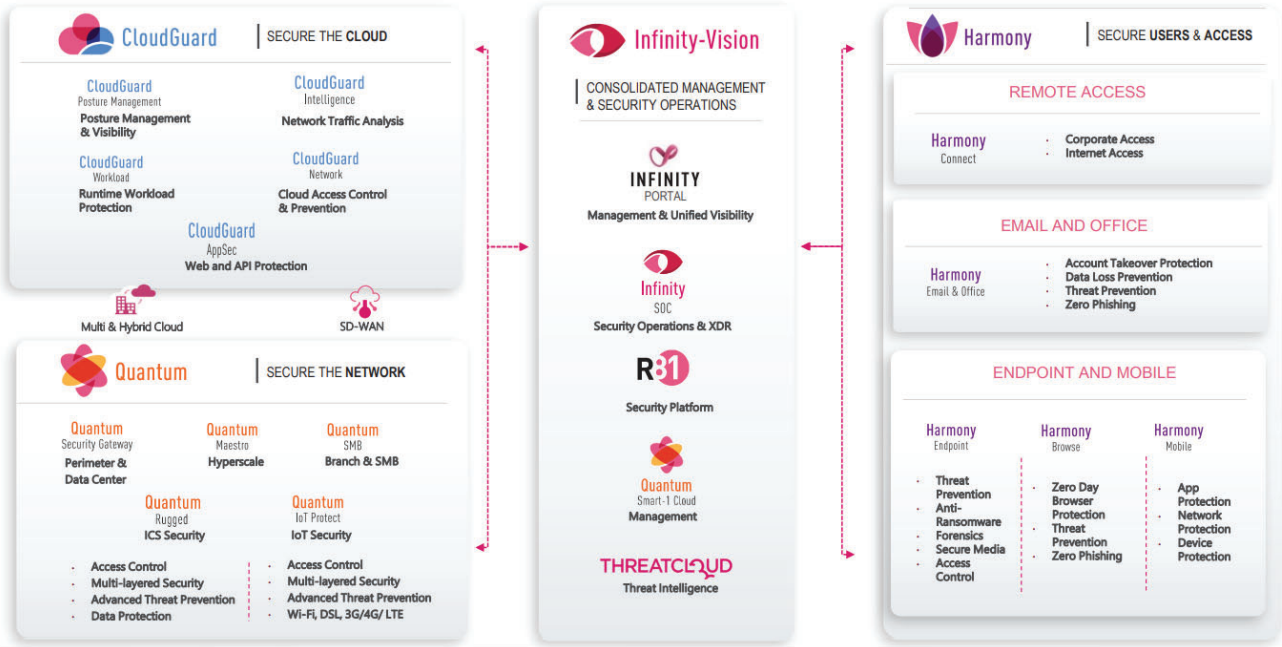
TRUSTED BY FORTUNE 500 COMPANIES

## 27 Years of Recognition

- Gartner** **Network:** 19th time Security Leader in Magic Quadrant
- Gartner** **Network:** Customers' Choice for Unified Threat Management
- NSS LABS** **Network:** Highest cyber prevention score in Breach Prevention
- M TEST** **Endpoint:** Top Product Scoring: 17.5 / 18
- FORRESTER** **Endpoint:** A leader in Endpoint Security
- IDC** **Mobile:** Highest Mobile security value
- Gartner** **Cloud:** Dome9, a cool vendor in Cloud Security



# THE MOST COMPLETE SECURITY



[Internal Use] for Check Point employees

## INTERESTING FACTS OF THIS CYBER WAR ...

### Hack Charge

MAY 10, 2022 / BY MI

### Cases of hac

As the world ra issues. The glc manufacturers reported that a display anti-wa station display: it could be a bi

Kremlin security agency to buy typewriters 'to avoid leaks'



THINKSTOCK

THINKSTOCK

### EV

ne major teething on the road, and as aimes. We recently an programmers to where charging commonplace, and

EUROP

Ha

Uk

By JOSI THE WA



## COMPROMISING MOBILE COMMUNICATIONS - TACTICS?



## HACKING A MOBILE PHONE (IPHONE) - TECHNIQUES...





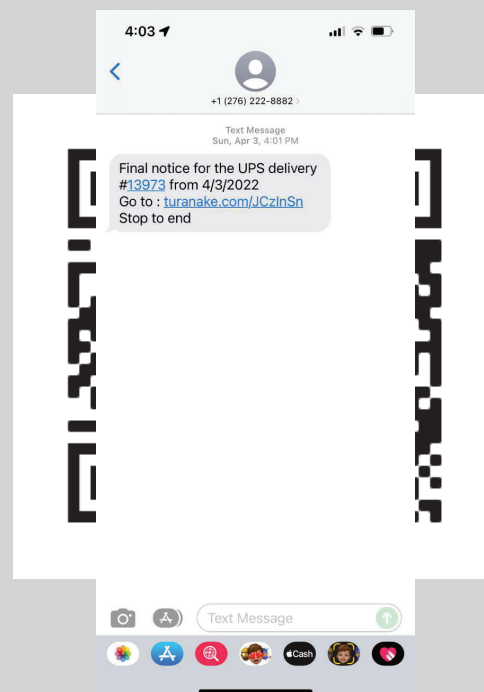
# COMPROMISING SYSTEMS VIA EMAILS - TACTICS?

## Multiple Hacker Groups Capitalizing on Ukraine Conflict for Distributing Malware

April 04, 2022 Ravi Lakshmanan



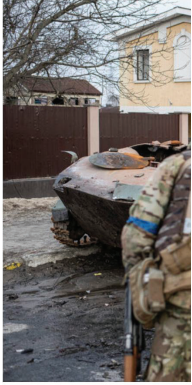
# HACKING VIA PHISHING - TECHNIQUES



# COMPROMISING ENDPOINTS - TACTICS?

## Despite hopes for peace, attacks increase in Ukraine conflict

Joe Uchill April 5, 2022



GuidePoint Security data shows ransomware attacks in Ukraine. Pictured: Members of territorial defense forces in Bucha, Ukraine. (Photo by Alexey Furman)

## Russian hackers start targeting Ukraine with Follina exploits

By Bill Toulas

June 13, 2022 10:28 AM 1



Ukraine's Computer Emergency Response Team (CERT) is warning that the Russian hacking group Sandworm may be exploiting Follina, a remote code execution vulnerability in Microsoft Windows Support Diagnostic Tool (MSDT) currently tracked as CVE-2022-30190.

## Microsoft

choice



Wedding might turn out to be the day of... a hacker's life

apienyte 18 June 2022

It might be a boom year for weddings. Romance also means millions of opportunities for hackers to ruin the celebration.

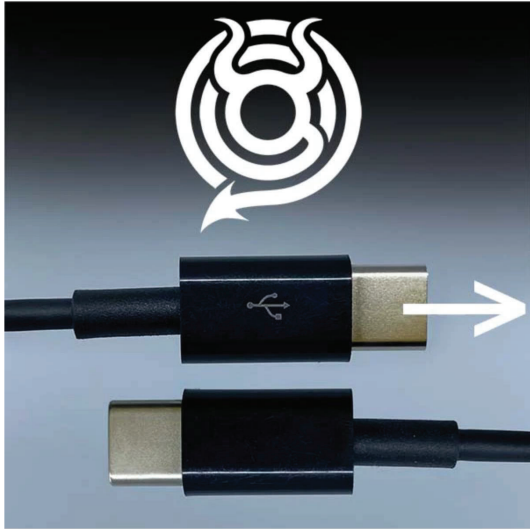
more

The curious case of Julian

# HACKING VIA HUMAN CURIOSITY - TECHNIQUES

PRODUCTS SHOWS PAYLOADS **HAK5** COMMUNITY SUPPORT





< PREVIOUS | NEXT >




**NEW**

### 0.MG CABLE - DIRECTIONAL

\$139.99

 <p>C TO C (BLACK) \$139.99</p>	 <p>C TO C + KEYLOGGER (BLACK) \$179.99</p>
 <p>C TO C (WHITE) \$139.99</p>	 <p>C TO C + KEYLOGGER (WHITE) \$179.99</p>

ACCESSORIES



A KEY WINNER OF THE WAR IN UKRAINE IS...

Forbes

CYBERSECURITY

ADVERTISEMENT

# iPhone 13 Pro Hacked: Chinese Hackers Suddenly Break iOS 15.0.2 Security

**Davey Winder** Senior Contributor   
Co-founder, Straight Talking Cyber

Follow

Oct 18, 2021, 06:01am EDT

including countries it considers friends.

## COMPROMISING IOS DEVICES (IPHONES)?

July 6, 2022

### Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware

Apple is previewing a groundbreaking security capability that offers specialized additional protection to users who may be at risk of highly targeted cyberattacks from private companies developing state-sponsored mercenary spyware. Apple is also providing details of its \$10 million grant to bolster research exposing such threats.



# LET'S PRETEND WE WANT TO HACK INTO AN ORGANIZATION USING: MALWARE AND PHISHING



DE98F96AFE650CF1CBC6C88AE59C8F11

## Threat Details Report

Actions ▾

Check Point



### clickme.docx

SIZE: 9.92 KB | TYPE: DOCX | [CVE-2021-40444](#) | [HASH list](#) ▾



Verdict  
Malicious

Action (Defined in Profile)  
Inactive



Confidence  
High



Secure / Risk  
Critical



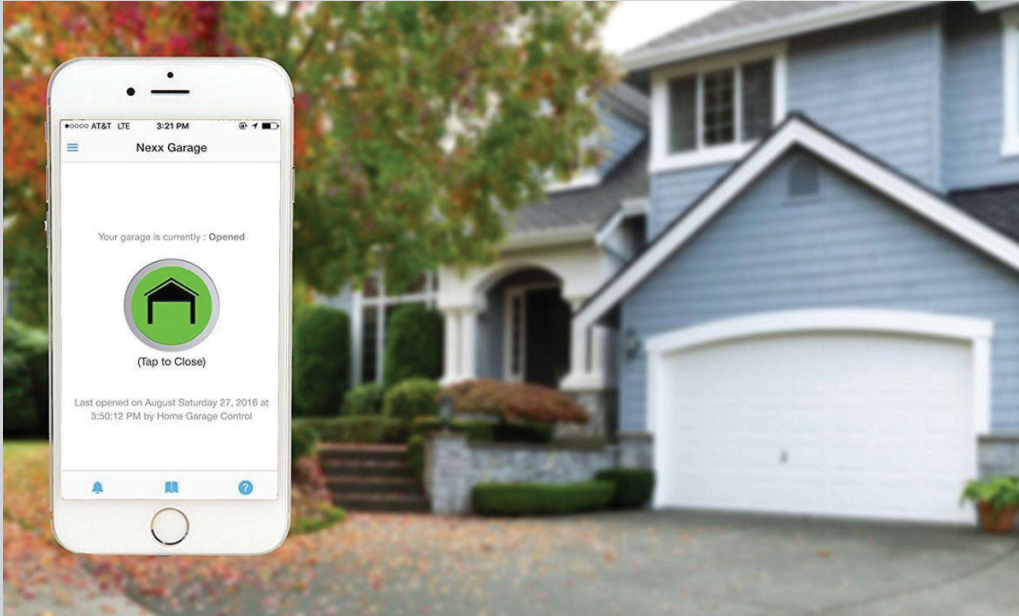
Classification  
Trojan

#### MITRE ATT&CK





INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION	COMMAND & CONTROL	IMPACT
	Execution through API	AppCert DLLs	AppCert DLLs	File Deletion	Exploitation For Credential Access	System Information Discovery	Remote Desktop Protocol	Email Collection	Data Encrypted	Commonly Used Port	Data Destruction
	Signed Binary Proxy Execution	Change Default File Association	Hooking	Signed Binary Proxy Execution	Steal Web Session Cookie	Application Window Discovery		Data from Local System	Exfiltration Over Command And Control Channel		
	Service Execution	Shortcut Modification		Virtualization / Sandbox Evasion	Credentials in Registry	Virtualization / Sandbox Evasion		Input Capture			
	Exploitation for Client Execution	Hooking			Input Capture						
					Hooking						

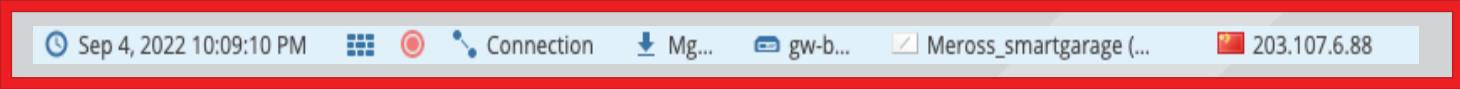
# MY SMART GARAGE DOOR VS CYBER WARFARE?



## SHOULD I TRUST MY SMARTGARAGE DOOR?...

APPLICATION	PACKAGE INFO	OS	ANALYSIS DATE	REPUTATION	PRIVACY	SECURITY	TOTAL SCORE
 meross	com.meross.meross 2.29.0/479 d80bf85470270663625d7b8c86acfded25cc677a0376a167c21		Mar 16 2022, 18:35:36	<div style="width: 68%;"><div style="background-color: #ffc107;">68%</div></div>	<div style="width: 49%;"><div style="background-color: #ffc107;">49%</div></div>	<div style="width: 66%;"><div style="background-color: #ffc107;">66%</div></div>	6.2

<b>Read External Storage Permission</b>	This application is allowed to read from the device's external storage. Files that are written to the external storage are readable by all other applications.	■■
<b>Access Precise Location Permission</b>	This application is allowed to access the device precise location.	■
<b>access location in the background Permis</b>	This application is allowed to access location in the background. (when not using the application)	■■
<b>Wifi networks Permission</b>	This application is allowed to access information about Wi-Fi networks.	■
<b>Access Approximate Location Permission</b>	This application is allowed to access the device approximate location.	■
<b>Camera Permission</b>	This application is allowed to get access to the device camera.	■
<b>Read system log permission</b>	This application is allowed to read the low-level system log files. Not for use by third-party applications, because Log entries can contain the user's private information.	■■■



# MY FAVORITE BUSINESS APP VS CYBER WARFARE?

## CamScanner - PDF Scanner App



CamSoft Information

Contains ads · In-app purchases

4.8★  
4.11M reviews

100M+  
Downloads

E  
Everyone

Install on more devices

Cloud Hosting Services



Firebase



LinkedIn



Google Drive



Microsoft OneDrive



Evernote



Baidu



VK



Twitter



Dropbox



Facebook



Google Cloud

# THE CYBER-CONFLICTS CONNECT ALL OF US...

THE VERGE

TECH

REVIEWS

SCIENCE

CREATORS

ENTERTAINMENT

VIDEO MORE



POLICY POLITICS

## The US has sanctioned the head of Russia's largest social network

2

Vladimir Kiriyenko, a Putin ally and son of a former prime minister, came to run VK Group after its founder was pushed out

By [Corin Faife](#) | [@corintxt](#) | Feb 26, 2022, 8:53am EST | 2 comments

### “People’s Liberation Army”: How Russia Still Uses VK To Influence Ukrainians

January 26, 2021

Although the popularity of the Russian social network VK in Ukraine has dropped, it is still being used to promote pro-Russian, anti-Western narratives in Ukraine.



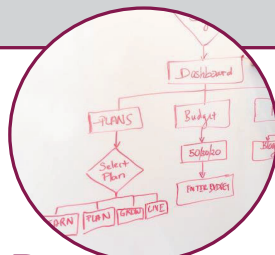
# SECURITY PRACTICES TO SECURE YOUR WORKFORCE

- *AVOID DANGER*
- *MINIMIZE RISKS*

## THE GOLDEN TRIANGLE (PPT)



**People**



**Processes**



**Technology**



## PEOPLE – MINIMIZING RISKS



## PEOPLE – AVOIDING DANGER

Mobile devices are they keys of our digital life

Security awareness training

Maintain a balance between usability vs security



# PROCESSES

The operational security model must be integrated into the business workflow



Pay attention on new trends such as BYOD (Bring your own environment)



To identify how sensitive data flows across systems and apply controls





# TECHNOLOGY

CYBER SCAPE

2021



# TECHNOLOGY

“Anyone who thinks that security products alone offer true security is settling for the illusion of security.”

— Kevin D. Mitnick

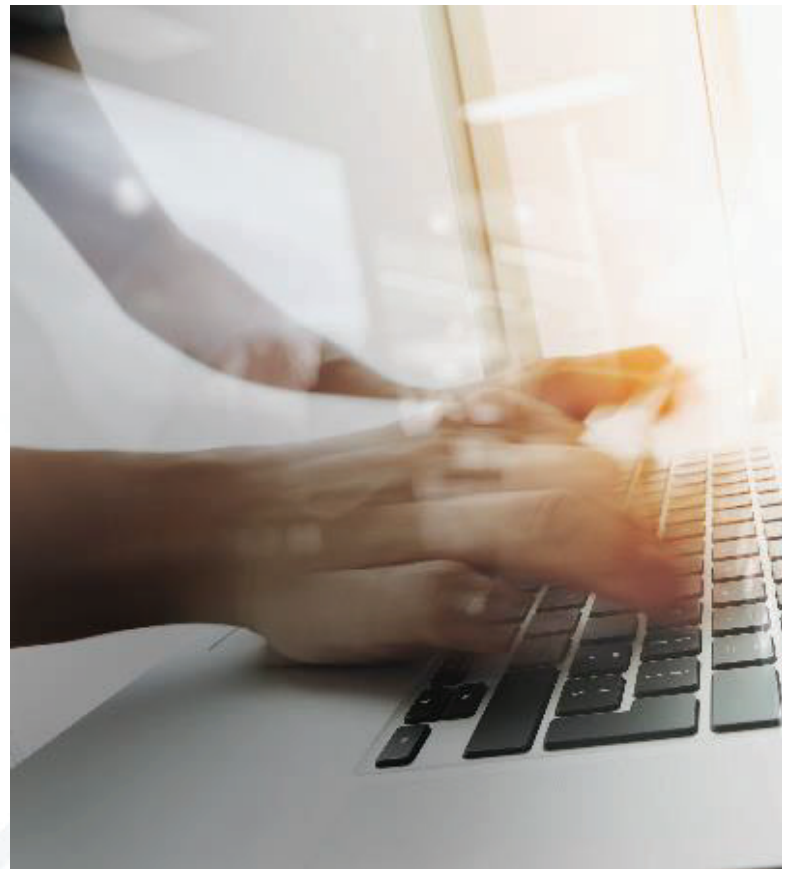
To  
summarize

- Hackers continuously find new ways to compromise organizations
- Pay attention to cyber security incidents happening overseas
- ***“In security, you are only as secure as the weakest link.” — Kevin D. Mitnick***



## CYBER TRENDS FROM THE WAR IN UKRAINE

Augusto Morales, PhD  
Technology Lead, Threat Solutions | Office of CTO  
Check Point Software Technologies  
IEEE Senior Member





# BACKUP

YOU DESERVE THE BEST SECURITY