

The 5G Battle



Presenters:

Bence D. Horvath CISM CISSP CRTIA

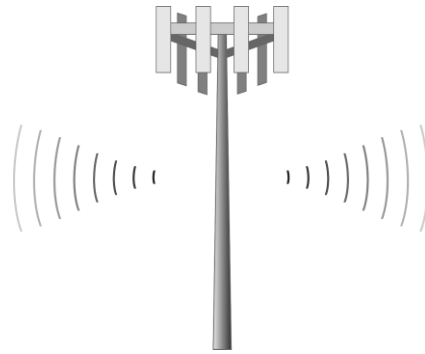
Robert A. Moody CISM CISA CRTIA

The Threat Landscape

- With the deployment of 5G infrastructure a unique threat landscape has arisen.



- Counter-5G activists propped up by conspiracy theories and nation state disinformation campaigns

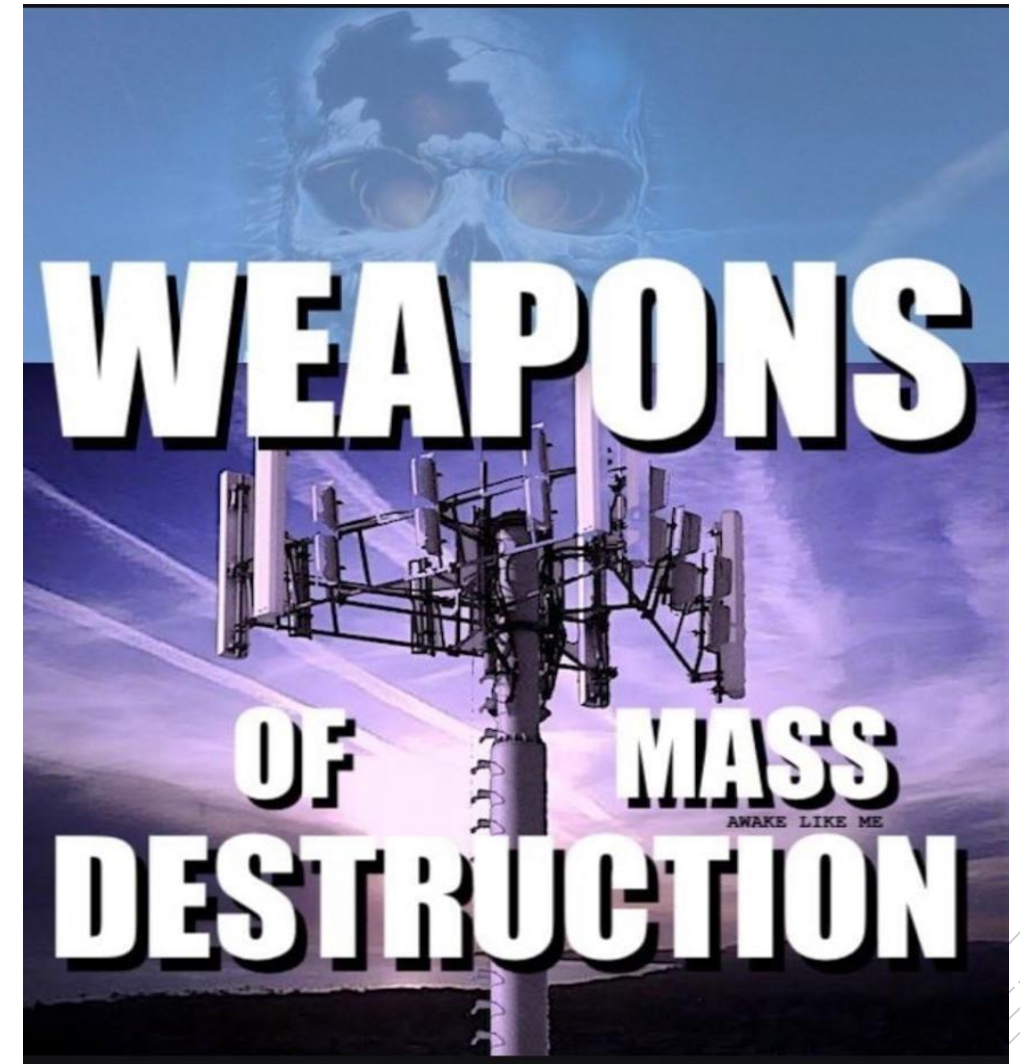


- “Traditional” high-threat actors who target the telecommunication and high tech sector, for a combination of political, diplomatic, SIGINT and monetary gains



- As well as corporate espionage, aimed primarily at stealing new technologies

Anti-5G Movement



Anti-5G News

5G coronavirus conspiracy theory leads to 77 mobile towers burned in UK, report says

Attacks on cell towers continue.

Caroline Reichert 17 May 7, 2020 9:31 a.m. PT



Mobile towers are being attacked in the UK due to false 5G coronavirus conspiracy theories. Caroline Reichert/ENET

For the most up-to-date news and information about the coronavirus pandemic, visit the [WHO website](#).


Almost 80 mobile towers have reportedly been burned down in the UK due to false coronavirus conspiracy theories that blame the spread of COVID-19 on 5G. The arson attacks began in early April, with 77 towers now damaged, Business Insider reported Wednesday citing industry group Mobile UK.

"Daily attacks are very low now but have not stopped entirely," a Mobile UK spokesman told Business Insider.

As of April 21, 40 employees of one UK carrier have also been attacked physically or verbally, according to BT CEO Philip Jensen. "We've even had one Openreach engineer stabbed and put in hospital," Jensen said.

Verschörungstheorien motivieren zu Anschlägen auf 5G-Masten

In Europa kommt es vermehrt zu Anschlägen auf 5G-Masten. Grund dafür sind Verschwörungstheorien, die Mobilfunkstrahlung für die Corona-Pandemie verantwortlich machen.

 Stephan Scheuer

24.04.2020 - 17:05 Uhr • [Kommentieren](#) • [3 x geteilt](#)

Funkmasten in Großbritannien wegen Coronavirus-Verschörungstheorie angezündet



Die Deutsche Telekom und Vodafone weiten massiv den Ausbau des Echtzeitmobilfunks in Deutschland aus. Schon heute ist klar, dass die Initiativen eine konkrete Konsequenz haben werden: Künftig wird es in Deutschland mehr Mobilfunkstandorte geben.

Schon in der Vergangenheit gab es Menschen, die Angst vor Mobilfunkstrahlung hatten. Getrieben von Verschwörungstheorien kommt es in immer mehr Ländern in Europa sogar zu gezielten Anschlägen auf Mobilfunkinfrastruktur.

[FEEDBACK](#)



Activist Actors

Priority Definition Planning	Priority Definition Direction	Target Selection	Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification	Adversary OPSEC	Establish & Maintain Infrastructure	Persona Development	Build Capabilities	Test Capabilities	Stage Capabilities
Create implementation plan	Task requirements	Determine approach/attack vector	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Analyze data collected	Assess targeting options	Analyze business processes	Anonymity services	Buy domain name	Build social network persona		Test physical access	Friend/Follow/Connect to targets of interest
Create strategic plan		Determine highest level tactical element	Conduct social engineering	Aggregate individual's digital footprint	Conduct social engineering			Assess security posture of physical locations	Network-based hiding techniques	Obfuscate infrastructure	Choose pre-compromised persona and affiliated accounts			
		Determine operational element	Identify job postings and needs/gaps	Conduct social engineering	Determine centralization of IT management				Obfuscate infrastructure		Develop social network persona digital footprint			
		Determine secondary level tactical element	Identify technology usage patterns	Identify groups/roles	Determine physical locations				Obfuscate operational infrastructure		Friend/Follow/Connect to targets of interest			
		Determine strategic target		Identify job postings and needs/gaps	Identify job postings and needs/gaps				Proxy/protocol relays					
				Identify people of interest	Identify supply chains				Secure and protect infrastructure					
				Identify personnel with an authority/privilege										
				Identify supply chains										
				Mine social media										

* The views expressed in this presentation are that of the speakers, and not reflective of their employers, customers, business partners, or private affiliations

Actors Targeting High-Tech and Telecommunication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	Command-Line Interface	Accessibility Features	Accessibility Features	Bypass User Account Control	Brute Force	Account Discovery	Exploitation of Remote Services	Automated Collection	Commonly Used Port	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File	Bootkit	Bypass User Account Control	Clear Command History	Credential Dumping	Network Service Scanning	Remote Desktop Protocol	Data from Local System	Connection Proxy	Data Encrypted	Resource Hijacking
Spearphishing Attachment	Exploitation for Client Execution	Create Account	DLL Search Order Hijacking	Code Signing	Input Capture	Network Share Discovery	Remote File Copy	Data Staged	Domain Generation Algorithms	Data Transfer Size Limits	
Supply Chain Compromise	PowerShell	DLL Search Order Hijacking	Exploitation for Privilege Escalation	Compiled HTML File		Process Discovery	Windows Admin Shares	Input Capture	Fallback Channels		
Valid Accounts	Regsvr32	External Remote Services	New Service	Connection Proxy		Query Registry	Windows Remote Management		Remote File Copy		
	Scheduled Task	Modify Existing Service	Process Injection	Deobfuscate/Decode Files or Information		Remote System Discovery			Standard Application Layer Protocol		
	Scripting	New Service	Scheduled Task	Disabling Security Tools		System Network Configuration Discovery			Web Service		
	Windows Management Instrumentation	Redundant Access	Valid Accounts	DLL Search Order Hijacking		System Network Connections Discovery					
	Windows Remote Management	Registry Run Keys / Startup Folder	Web Shell	DLL Side-Loading		System Owner/User Discovery					
		Scheduled Task		File Deletion							
		Valid Accounts		Hidden Window							
		Web Shell		Indicator Removal from Tools							
				Indicator Removal on Host							
				Masquerading							
				Modify Registry							
				Network Share Connection Removal							
				Obfuscated Files or Information							
				Process Injection							
				Redundant Access							
				Regsvr32							
				Rootkit							
				Scripting							
				Valid Accounts							
				Web Service							

* The views expressed in this presentation are that of the speakers, and not reflective of their employers, customers, business partners, or private affiliations

Espionage Actors

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Replication Through Removable Media	Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Automated Collection	Commonly Used Port	Data Compressed	
Spearphishing Attachment	Dynamic Data Exchange	Bootkit	Accessibility Features	Bypass User Account Control	Input Capture	Network Service Scanning	Logon Scripts	Data from Information Repositories	Communication Through Removable Media		
Spearphishing Link	Exploitation for Client Execution	Component Object Model Hijacking	Bypass User Account Control	Component Object Model Hijacking	Network Sniffing	Network Sniffing	Pass the Hash	Data from Local System	Connection Proxy		
Trusted Relationship	PowerShell	Hidden Files and Directories	Exploitation for Privilege Escalation	Connection Proxy		Peripheral Device Discovery	Pass the Ticket	Data from Removable Media	Custom Cryptographic Protocol		
Valid Accounts	Rundll32	Logon Scripts	Scheduled Task	Deobfuscate/Decode Files or Information		Process Discovery	Remote Desktop Protocol	Data Staged	Data Obfuscation		
Hardware Additions	Scheduled Task	Office Application Startup	Valid Accounts	Exploitation for Defense Evasion		System Network Configuration Discovery	Remote File Copy	Email Collection	Domain Fronting		
	Scripting	Registry Run Keys / Startup Folder	Web Shell	File Deletion		System Owner/User Discovery	Remote Services	Input Capture	Multi-hop Proxy		
	User Execution	Scheduled Task		Hidden Files and Directories			Replication Through Removable Media	Screen Capture	Remote File Copy		
	Windows Management Instrumentation	Shortcut Modification		Hidden Window					Standard Application Layer Protocol		
		Valid Accounts		Indicator Removal on Host					Standard Non-Application Layer Protocol		
		Web Shell		Obfuscated Files or Information							
		Windows Management Instrumentation Event Subscription		Rootkit							
				Rundll32							
				Scripting							
				Software Packing							
				Template Injection							
				Timestamp							
				Valid Accounts							

* The views expressed in this presentation are that of the speakers, and not reflective of their employers, customers, business partners, or private affiliations

Applying the Matrices

CTI

- With the insights gained on potential actor activity CTI teams can operationalize this information to actively monitor clear, deep and dark web sources for:
 - Indicators of attack or intent to attack,
 - Social media campaigns targeting their organizations
 - New campaigns for specific threat actor groups
 - Exposed infrastructure or user accounts that can be used by an actor as part of Initial Access

Red Team

- With the insights gained on potential actor activity Red Teams can leverage this information to build realistic test scenarios:
 - The flags used in campaigns can be aligned with the TTPs that threat actors have been observed using in previous attacks
 - The Impact and Exfiltration techniques can be aligned with the TTPs that threat actors have been observed previously, allowing the organization to see how they would respond in the event of an APT attack

Blue Team

- With the insights gained on potential actor activity Blue Teams can:
 - Create more advanced SOC Use Cases, enhancing detection capabilities:
 - Identify gaps in preventative coverage and in log sources
 - More rapidly detect anomalous activity
 - Stop advanced attack methodologies sooner in their progression

White Team

- With the insights gained on potential actor activity management and senior stakeholders are informed of the shifts in the threat landscape, and can make decisions for preempt investment, law enforcement involvement, and public relations.

Speaker Bios

Robert Moody is a cyber threat intelligence and digital forensics expert, currently working as a Threat Intelligence Officer at Telefónica Germany.

He has a background working in critical infrastructure sectors including telecommunication, manufacturing, banking, finance, and energy.

He has a Masters in Cybersecurity from ie University, and holds Certified Information Security Manager (CISM), Certified Information System Auditor (CISA), and Crest Registered Threat Intelligence Analyst (CRTIA) qualifications.

LinkedIn: <https://www.linkedin.com/in/robert-a-moody-1aa624153/>



Bence Horvath is a seasoned cybersecurity executive focused on next-generation cyber defence and intelligence-led offensive operations.

He currently leads the Advanced Security Testing Practice for EY's Cybersecurity Advisory in London, focused on Tier 1 clients in the financial services and CNI sectors.

His background includes working in telecommunication, aerospace and defence, financial services and consulting. He has an MBA from ie Business School, an M.Sc. in Business Information Systems from the Corvinus University, and holds CRTIA, CISSP and CISM certifications.

LinkedIn: <https://www.linkedin.com/in/bencehorvath/>

