CRASHOVERRIDE: The Malware That Attacks Power Grids

JANUARY 10, 2018 • MONICA TODROS

Editor's Note*: The following blog post is a summary of a presentation from RFUN 2017 featuring Robert M. Lee, CEO and founder at Dragos.*

Key Takeaways

- With the recent increase of different attackers, methodologies, and adversaries that can affect industrial control systems, what once was never a concern, now is.
- Energy companies and other industrial companies have been targeted in the past, but there just wasn't any adequate incident response available to properly react.
- The CRASHOVERRIDE malware framework successfully disrupted power in one site and hit a sweet spot of scalability that deserves attention

scalability that deserves attention. Threat intelligence is much farther reaching than indicators of compromise and leveraging intelligence on the CRASHOVERRIDE attack, it also helps you understand what you are looking for following detection, and in the future.

Industrial control systems (ICS) are complex infrastructures, making it difficult for adversaries who gain access to cause far-reaching impact.

While compromising ICS security is not as difficult as the industry would like, causing significant and widescale disruption is significantly harder than people make it out to be. Just take a look at the electric grid — it's the biggest living ecosystem ever designed.

Some attackers, however, are up for the challenge.

Robert M. Lee, CEO and founder at Dragos, recently spoke at Recorded Future's annual user conference in D.C. to share both his deep expertise on industrial control systems, and details of his investigation into the most impactful ICS malware attack to date, CRASHOVERRIDE.

This malware targeted toward industrial control systems is specifically crafted to be an attack framework. Lee emphasizes that instead of over-focusing threat intelligence on the indicators involved, it should be focused on the behavior of the attack and what to do about it.

The malware itself scales very well and focuses not on vulnerabilities and exploits, but on leveraging legitimate grid operations against itself. For this reason, once CRASHOVERRIDE or capabilities like it are in place, there's limited options. You have to keep the adversaries out and know what to do about them for when that strategy fails.

Adversaries at Work

Let's back up for a moment. While the CRASHOVERRIDE framework took down a transmission-level substation in Ukraine in 2016, the world actually saw the first transmission-level substation in Ukraine in 2016, the world actually ever power outage due to a cyberattack one year prior, also occur BlackEnergy 3 received a lot of news activity and buzz as the malware involved, but this particular malware did not cause the outages.

Lee says that the most interesting element of the 2015 malware attack was the human operators — an estimated 20 people involved, given the forensics and timing of keyword actions. And interestingly enough, those involved just went ahead and picked up knowledge on industrial operations to execute the attack.

So, malware didn't take down the power grid, Lee explains. It was the adversaries learning how to control industrial control systems and using them for exactly what they're built for: turning on and off power. Knowing this, the motivations and behaviors behind this attack mattered a lot more than any indicators or digital hashes.

In the IT community, there are a multitude of big companies that have endpoint protection, intrusion detection systems, and firewalls that report back to them. That is a big difference in the threat landscape between ICS and IT. Traditionally, industrial control systems have not had security technologies connected to the internet beaconing back to companies when it sees things, and with good reason, Lee states. In fact, many antivirus programs would actually cause more damage to an industrial control system environment than it would fix.

There is a lot of visibility in IT, which over time has unfolded in different shapes and sizes. Threat intelligence has built up over the years, and there has been a significant amount of intrusions into those environments. With industrial control systems, that data collection has never taken place. Not until recent years, that is.

There is a multitude of different attackers, methodologies, and adversaries out there that can affect ICS, some of which would have never been understood or even discovered without thorough analysis, or in Lee's case, a mission designed specifically for the matter.

Going on a Mission

In Lee's previous career, he built the National Security Agency's mission for identifying and analyzing nation states breaking into industrial environments. What

identifying and analyzing nation states breaking into industrial envi
Lee found at the time shocked him: nation-state cyber teams he h
before. Specifically, the first ever African nation-state cyber operations team breaking into governments and industrial sites in other places.

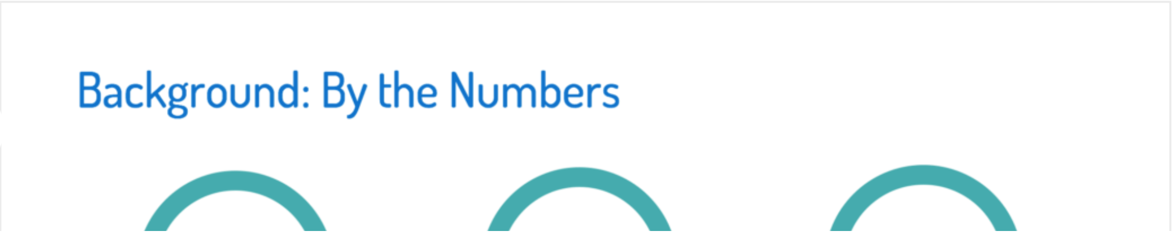
Lee started identifying a multitude of different methodologies of attacks and found that attackers were compromising big industrial vendors, going in through the VPNs (virtual private networks) into the industrial control systems. The methodologies, the trade craft, and the adversaries were different, and that was exciting, Lee explains. It was new for him to try and figure out what that might actually mean for the community. Years later, Lee would leave the NSA and found Dragos, Inc., including members of his old team.

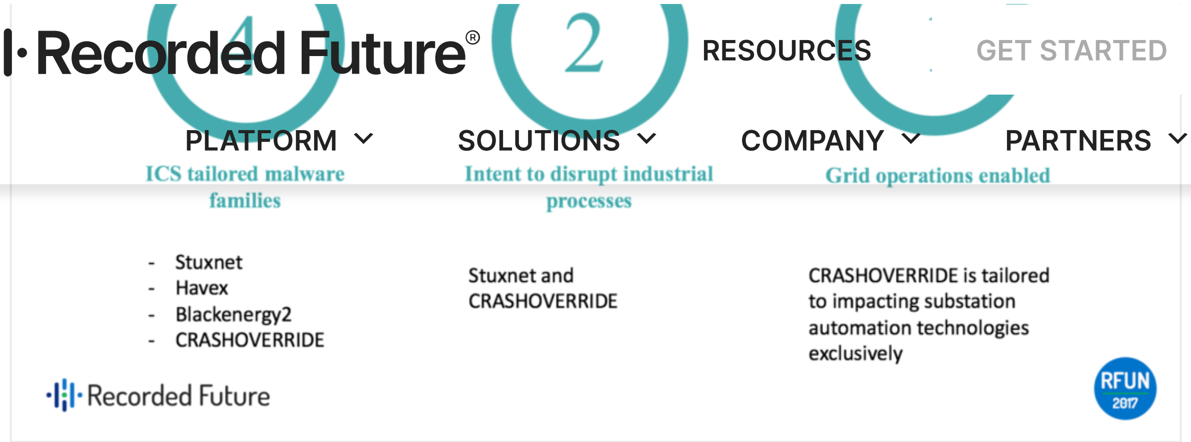
When investigating the 2015 attack, Lee recognized that even with attribution, the case would be politically difficult. Much to his dismay, even after advising the White House and others on the event, it was let go and there was no official response. That was the first time somebody turned off the lights through a cyberattack. Unsatisfied with this lack of response, Lee believed this was a missed opportunity to set the precedent for attacking civilian infrastructure.

Regardless of government involvement, however, the civilian community still had to deal with the reality of the attack. Lee noted many of the industrial companies went above and beyond to start preparing, training, and coordinating on how to respond to such attacks.

Malware by the Numbers

To date, there have only ever been four pieces of malware specifically tailored for ICS, as shown in the image below, but there have been a lot of campaigns targeting industrial infrastructure.





ICS tailored malware families

- Stuxnet
- Havex
- Blackenergy2
- CRASHOVERRIDE

Intent to disrupt industrial processes

Stuxnet and CRASHOVERRIDE

Grid operations enabled

CRASHOVERRIDE is tailored to impacting substation automation technologies exclusively

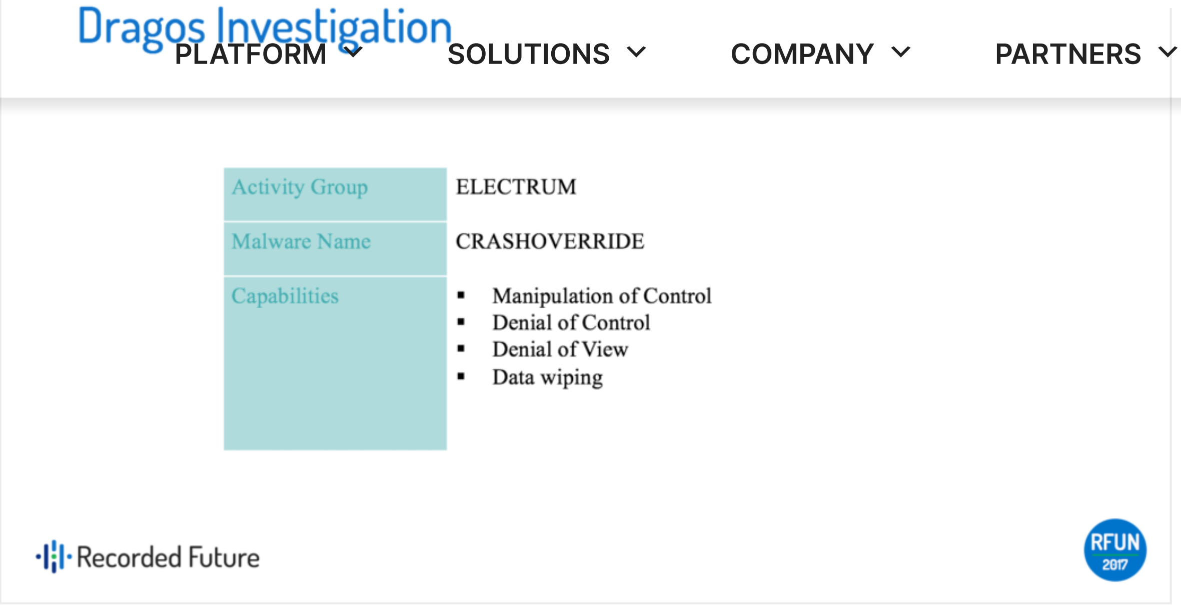
Industrial companies have been targeted in the past, but there just wasn't adequate incident response available to properly react and codify lessons learned, as well as document knowledge on the threats. Without the necessary incident response, any opportunities to become better as a community by learning from the adversaries were not taken.

As far as ICS-tailored malware, it's an interesting type of attack, Lee states. It's difficult to do things with complex environments using industrial control systems, and not because you can't figure out the protocols or because a control system is weird, but because the physical implementation and engineering of the systems can be entirely unique site to site. It's not an aspect of the adversary not being able to accomplish an attack, but instead, it's a challenge of disruption and scalability.

Assessing the Damage

So, what happened in Ukraine? Essentially, the CRASHOVERRIDE malware framework was able to codify grid operations knowledge and lessons learned from 2015. Without focusing on vulnerabilities and exploits, it could be leveraged in sites around the world with little-to-no tailoring. However, there's still human operations that would have to be run to put it in place, so there was no need to start panicking.

Additionally, while the scalability is enormous, the impact is not as significant as some would fear. In Kiev, Ukraine, the outage lasted only about an hour. On the malware's impact, Lee says, "The interesting thing with CRASHOVERRIDE is it hits that nice little sweet spot. We've got something that's actually really, really scalable, but something that's not going to physically destroy equipment or be a long impact, yet, it's still disruptive."



Dragos Investigation

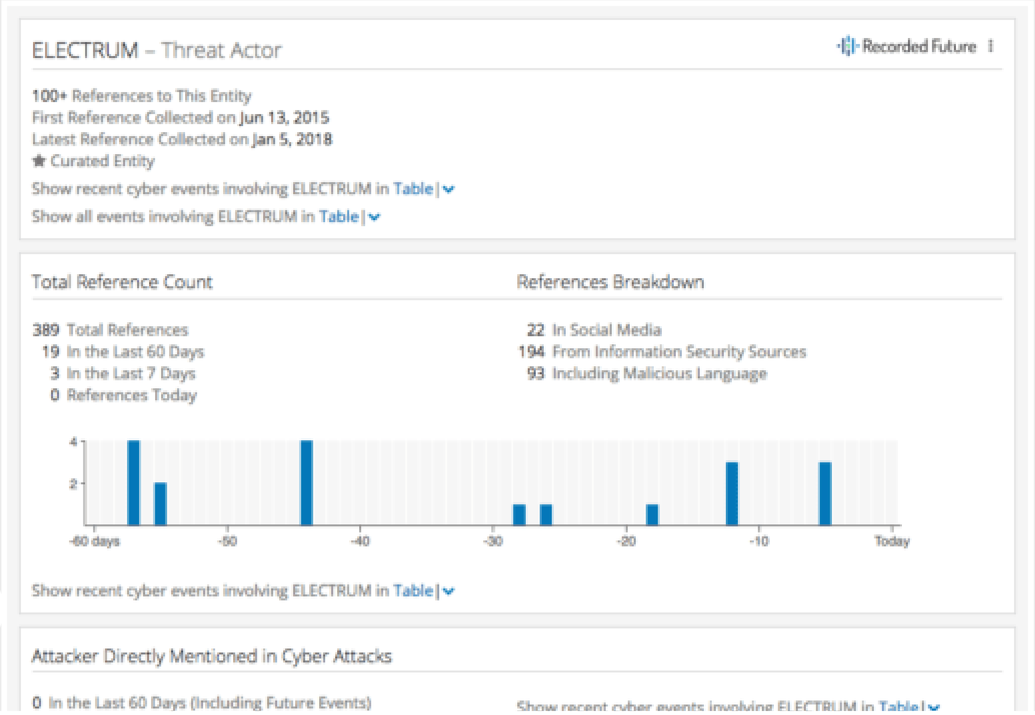
Activity Group	ELECTRUM
Malware Name	CRASHOVERRIDE
Capabilities	▪ Manipulation of Control ▪ Denial of Control ▪ Denial of View ▪ Data wiping

Recorded Future

RFUN 2017

During the investigation, Lee wanted to go a little bit deeper than the malware piece and focus on the adversaries — specifically, on the fact that it was a targeted threat group behind the operation.

The ELECTRUM threat actor group didn't actually conduct the operation, though they were responsible for developing the CRASHOVERRIDE framework. Evidently, the team that conducted the operation against the Kiev transmission-level substation in 2016 — effectively taking down the power station — was the Sandworm group, Lee's findings showed.



ELECTRUM – Threat Actor

Recorded Future

100+ References to This Entity
First Reference Collected on Jun 13, 2015
Latest Reference Collected on Jan 5, 2018
★ Curated Entity

Show recent cyber events involving ELECTRUM in Table |

Show all events involving ELECTRUM in Table |

Total Reference Count

389 Total References
19 In the Last 60 Days
3 In the Last 7 Days
0 References Today

References Breakdown

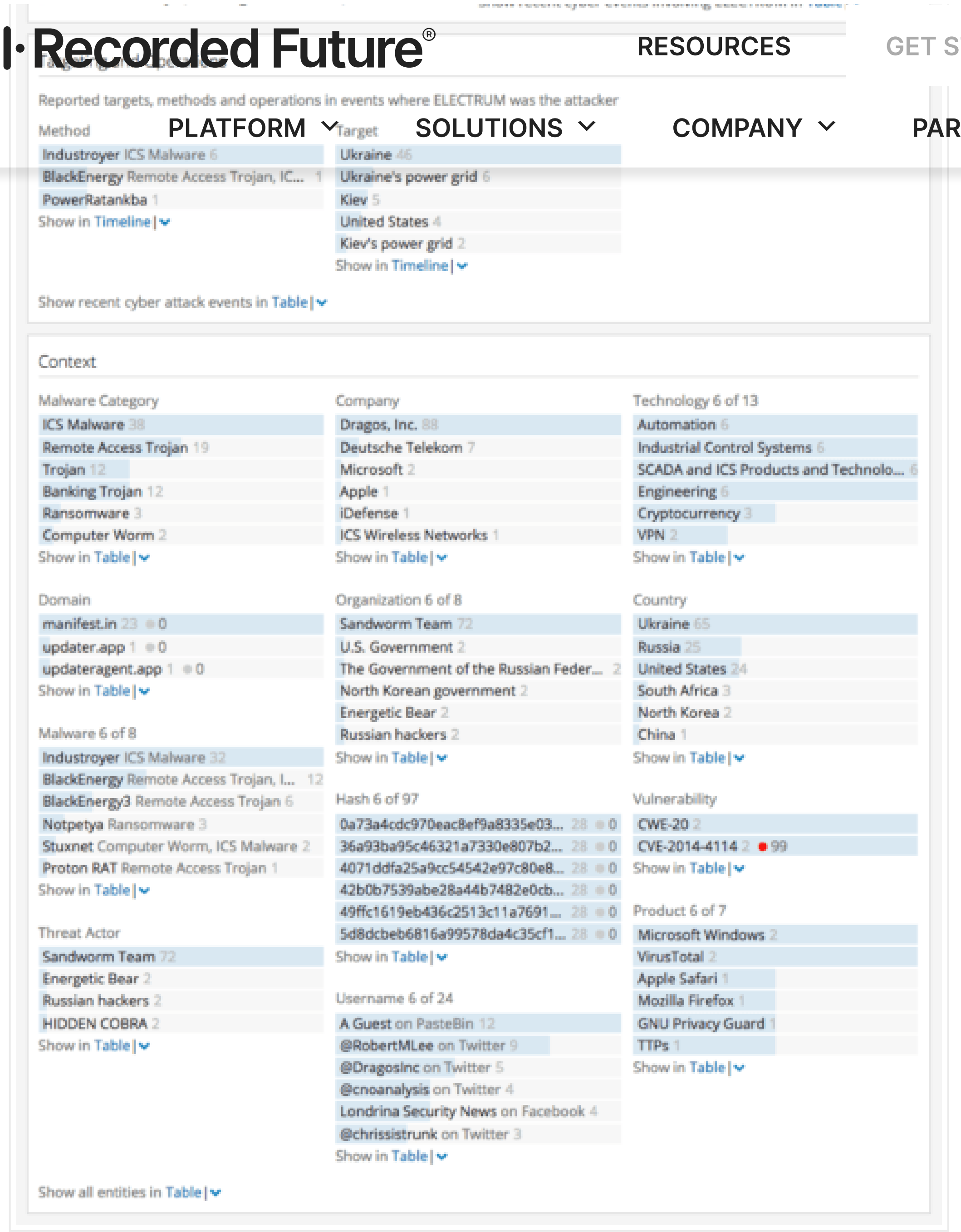
22 In Social Media
194 From Information Security Sources
93 Including Malicious Language

Show recent cyber events involving ELECTRUM in Table |

Attacker Directly Mentioned in Cyber Attacks

0 In the Last 60 Days (Including Future Events)

Show recent cyber events involving ELECTRUM in Table |



Targeting and Operations

Reported targets, methods and operations in events where ELECTRUM was the attacker

Method
Industroyer ICS Malware 6
BlackEnergy Remote Access Trojan, IC... 1
PowerRatankba 1
Show in Timeline |

Target
Ukraine 46
Ukraine's power grid 6
Kiev 5
United States 4
Kiev's power grid 2
Show in Timeline |

Show recent cyber attack events in Table |

Context

Malware Category
ICS Malware 38
Remote Access Trojan 19
Trojan 12
Banking Trojan 12
Ransomware 3
Computer Worm 2
Show in Table |

Domain
manifest.in 23 ● 0
updater.app 1 ● 0
updateragent.app 1 ● 0
Show in Table |

Malware 6 of 8
Industroyer ICS Malware 32
BlackEnergy Remote Access Trojan, I... 12
BlackEnergy3 Remote Access Trojan 6
Notpetya Ransomware 3
Stuxnet Computer Worm, ICS Malware 2
Proton RAT Remote Access Trojan 1
Show in Table |

Threat Actor
Sandworm Team 72
Energetic Bear 2
Russian hackers 2
HIDDEN COBRA 2
Show in Table |

Company
Dragos, Inc. 88
Deutsche Telekom 7
Microsoft 2
Apple 1
iDefense 1
ICS Wireless Networks 1
Show in Table |

Organization 6 of 8
Sandworm Team 72
U.S. Government 2
The Government of the Russian Feder... 2
North Korean government 2
Energetic Bear 2
Russian hackers 2
Show in Table |

Hash 6 of 97
0a73a4cdc970eac8ef9a8335e03... 28 ● 0
36a93ba95c46321a7330e807b2... 28 ● 0
4071ddfa25a9cc54542e97c80e8... 28 ● 0
42b0b7539abe28a44b7482e0cb... 28 ● 0
49ffc1619eb436c2513c11a7691... 28 ● 0
5d8dcbeb6816a99578da4c35cf1... 28 ● 0
Show in Table |

Username 6 of 24
A Guest on PasteBin 12
@RobertMLee on Twitter 9
@DragosInc on Twitter 5
@cnoanalysis on Twitter 4
Londrina Security News on Facebook 4
@chrissistrunk on Twitter 3
Show in Table |

Technology 6 of 13
Automation 6
Industrial Control Systems 6
SCADA and ICS Products and Technolo... 6
Engineering 6
Cryptocurrency 3
VPN 2
Show in Table |

Country
Ukraine 65
Russia 25
United States 24
South Africa 3
North Korea 2
China 1
Show in Table |

Vulnerability
CWE-20 2
CVE-2014-4114 2 ● 99
Show in Table |

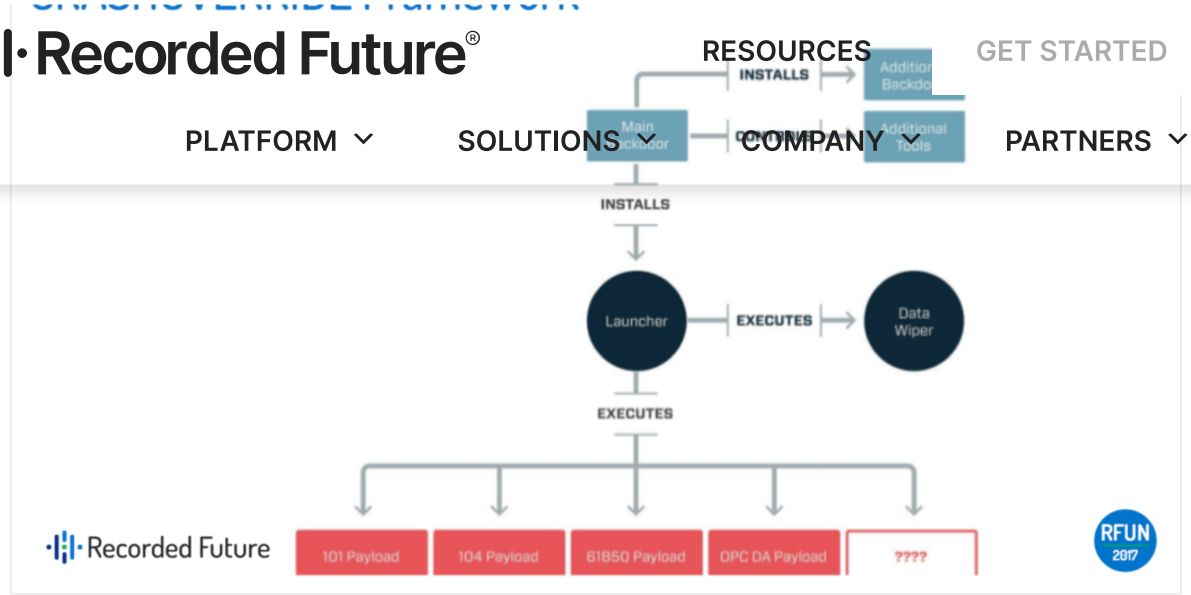
Product 6 of 7
Microsoft Windows 2
VirusTotal 2
Apple Safari 1
Mozilla Firefox 1
GNU Privacy Guard 1
TTPs 1
Show in Table |

Show all entities in Table |

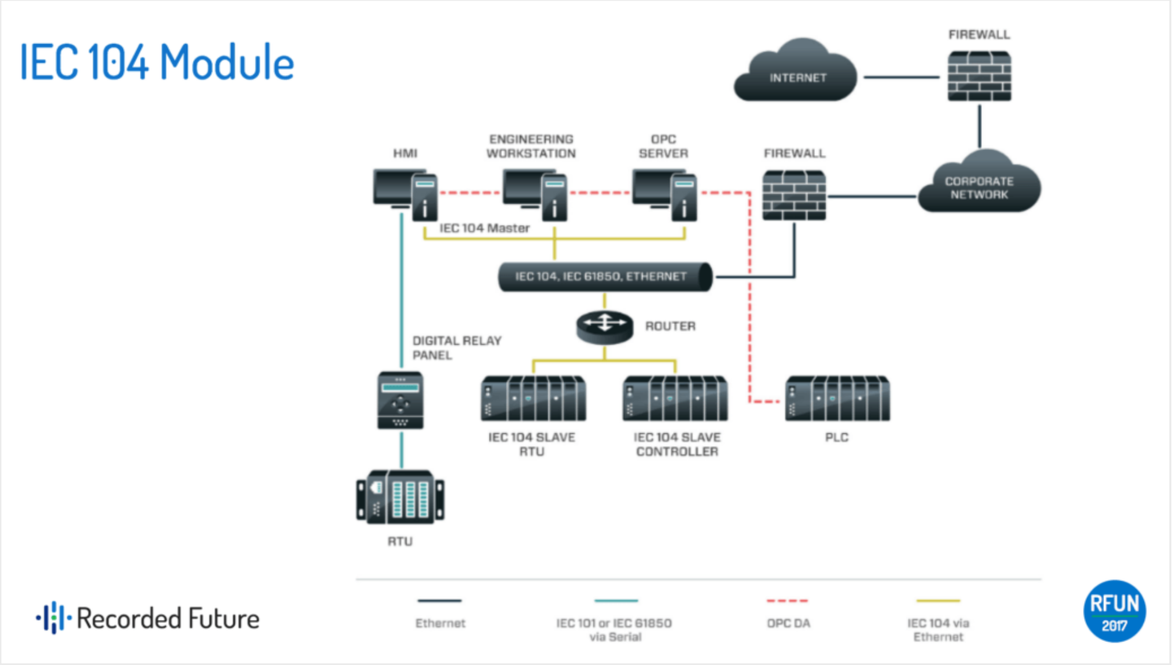
The Recorded Future Intelligence Card™ for ELECTRUM provides context around the attack.

It was discovered that the malware does manipulate data streams and data control, but it doesn't destroy things. In essence, all it did was learn how grids work and use that knowledge to disrupt. The downside of this? "There's no patch for CRASHOVERRIDE. There's no fix for it. If it's in place, or its tradecraft is in place, then your lights are going out. What you do about that before and after its occurrence is what matters," Lee explains.

CRASHOVERRIDE Framework



Looking at the framework itself, it has some things that you would expect on the IT side: launchers, back doors, the ability to delete files off the system. At the bottom of the image above, you can see the protocols listed out that work in European electric grids, including IEC 104, IEC 101, 61850, and OPC. The interesting thing about these protocols is that you actually don't need all of them for an attack, Lee explains. For this reason, Lee and his team assessed that this attack was more of a test case than the ultimate objective.



For a successful attack, only one protocol was actually needed to occur and interact with the systems: IEC 104. All of the other protocols were just development frameworks, meant for building a scalable framework that can operate in the places that attackers go. The adversary didn't have to go through a significant intel gain loss consideration with CRASHOVERRIDE, Lee states. There's no fixing the tradecraft, because it works based on how electric grids are run.

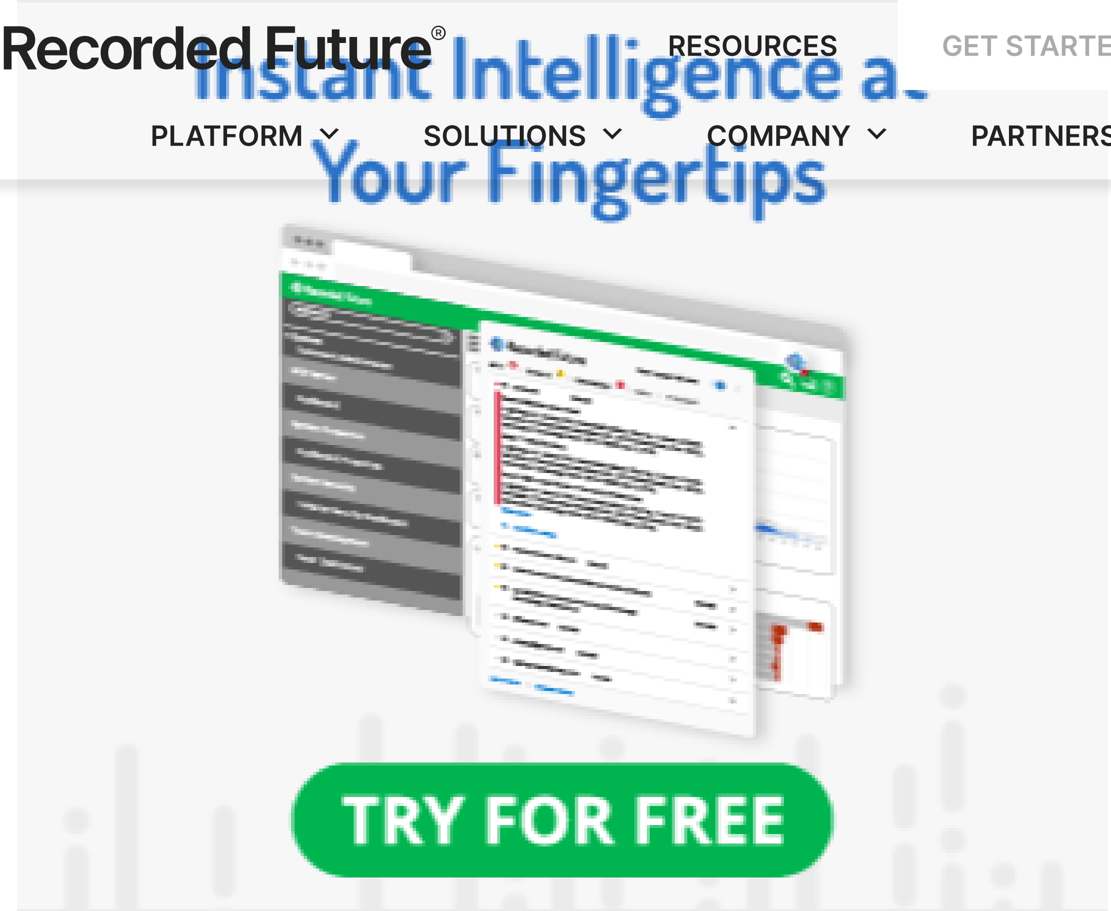
Action Points

It's not that threat intelligence led to detection of this impactful attack, it's that after detection, threat intelligence was available to help understand what you were looking at, Lee concludes.

The world has now seen two instances in history when a power grid has failed due to a cyberattack; one that was not very scalable, and one where it was not only scalable, but also provided adversaries with new knowledge. "Both times, no senior-level leader in any Western government has come out and condemned the attack. As intelligence professionals, we have to figure out why," Lee says.

Maybe this doesn't matter immediately in your organization, but it's not about how you can produce the intel that you like — it's about sticking to the true narrative. The industrial control system community is taking action to let people understand that the threat intelligence being done has national impacts, so it's important to stay informed in your own security strategy.

If you're interested in learning more about how threat intelligence can positively impact your organization and help defend against threats, contact us for a personalized demo.



Categories

- COMPANY
- CYBER THREAT INTELLIGENCE
- GEOPOLITICAL INTELLIGENCE
- OPINION
- PODCAST
- PRODUCT
- RESEARCH
- VULNERABILITY MANAGEMENT

POPULAR

How Predict 2020 Disrupted the Status Quo
OCTOBER 9, 2020

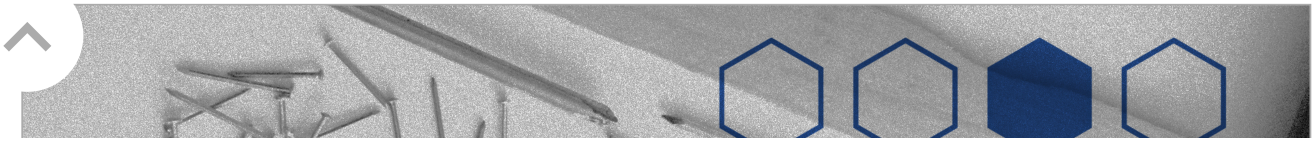
What Is SecOps Intelligence?
OCTOBER 7, 2020

What Brand Intelligence Means for Your Organization
OCTOBER 6, 2020

4 Things Nobody Tells You About Security Intelligence
SEPTEMBER 23, 2020

5 Questions to Ask Yourself About Your Third-Party Risk
SEPTEMBER 16, 2020

Related Posts

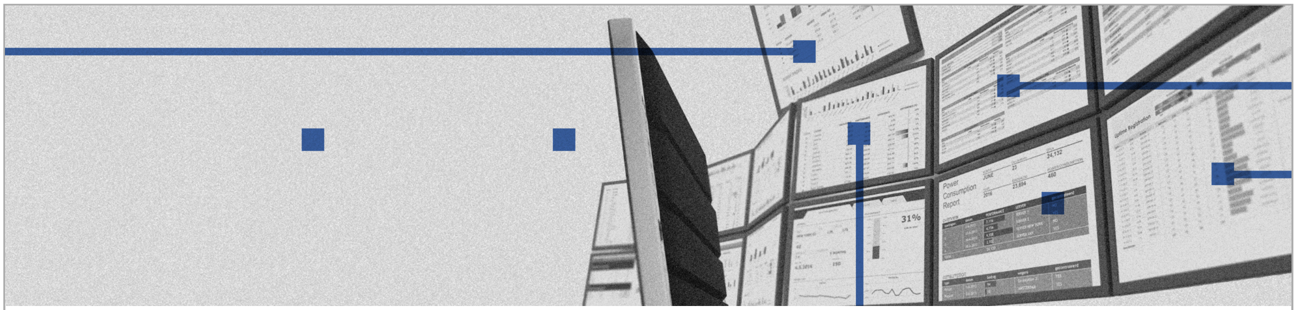


How ManoMano Defends Against Underground Data Marketplaces With Elite Security Intelligence

OCTOBER 14, 2020 • THE RECORDED FUTURE TEAM

ManoMano, Europe's leading marketplace for do-it-yourself home improvement and gardening...

READ MORE →



What Is SecOps Intelligence?

OCTOBER 7, 2020 • THE RECORDED FUTURE TEAM

Security operations and incident response teams operate under enormous pressure As their...

READ MORE →

What Brand Intelligence Means for Your Organization

OCTOBER 6, 2020 • THE RECORDED FUTURE TEAM

Protecting your brand doesn’t stop at securing your network or systems Digital risk to your brand…

READ MORE →

PLATFORM

Overview
Security Intelligence Graph
Interaction Points
Integrations
Services
License Options

SOLUTIONS

Brand Intelligence
SecOps Intelligence
Threat Intelligence
Vulnerability Intelligence
Third-Party Intelligence
Geopolitical Intelligence

PARTNERS

Overview
VAR
Technology
MSSP
OEM

COMPANY

About
Clients
Events
Press
Careers
Contact

RESOURCES

Blog
Cyber Daily
Handbook
Videos
Podcasts
Reports
Webinars

INFORMATION

Cookies
FAQ
Sign In
Privacy
Support
Terms