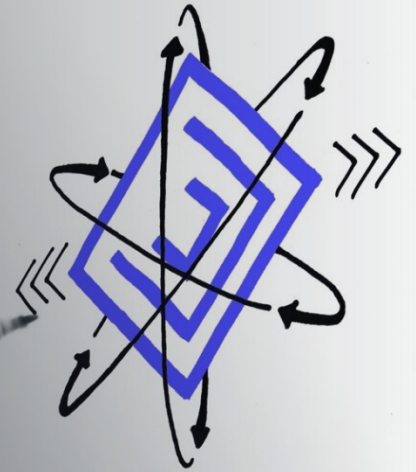




# Zeroing In On XENOTIME: Analysis Of The Entities Responsible For The Triton Event

Joe Slowik  
VB2022



# WHOAMI

---

- Current:
  - Gigamon: CTI & Detections Lead
- Previously:
  - DomainTools, Dragos: CTI Research
  - Los Alamos National Laboratory: IR Lead
  - US Navy: *Stuff*



---

# Agenda

1. The Triton Event
2. Post-Triton Activity
3. Examining Responsibility
4. Developers, Actors, and Operators
5. Complex Attribution Concerns



<https://cdn.costumewall.com/wp-content/uploads/2017/10/king-Triton.jpg>

# Triton/TRISIS/HatMan

The Triton Event

**E&E NEWS | ENERGYWIRE**      Publications ▾    Our Newsroom ▾    About ▾    Events    **LOGIN**    **GET ACCESS**    🔍

## The inside story of the world's most dangerous malware

By Blake Sobczak | 03/07/2019 07:20 AM EST



Claudine Hellmuth/E&E News(Illustration); Kremlin/Wikipedia(Putin); Xiquinho Silva/Flickr(St Basil Cathedral); FireEye (logo, hacker code graphics); perlishaper/Wikipedia(globe)

# Triton/TRISIS/HatMan

The Triton Event

**MANDIANT** Platform Solutions Intelligence Services Resources Company

THREAT RESEARCH

## Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure

BLAKE JOHNSON, DAN CABAN, MARINA KROTOFIL, DAN SCALI, NATHAN BRUBAKER, CHRISTOPHER GLYER

DEC 14, 2017 | 14 MINS READ

#MALWARE


**DRAGOS**

Whitepaper

## TRISIS: Analyzing Safety System Targeting Malware

By Robert M. Lee 12.14.17



 **CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**

CISA.gov Services Report

Alerts and Tips Resources

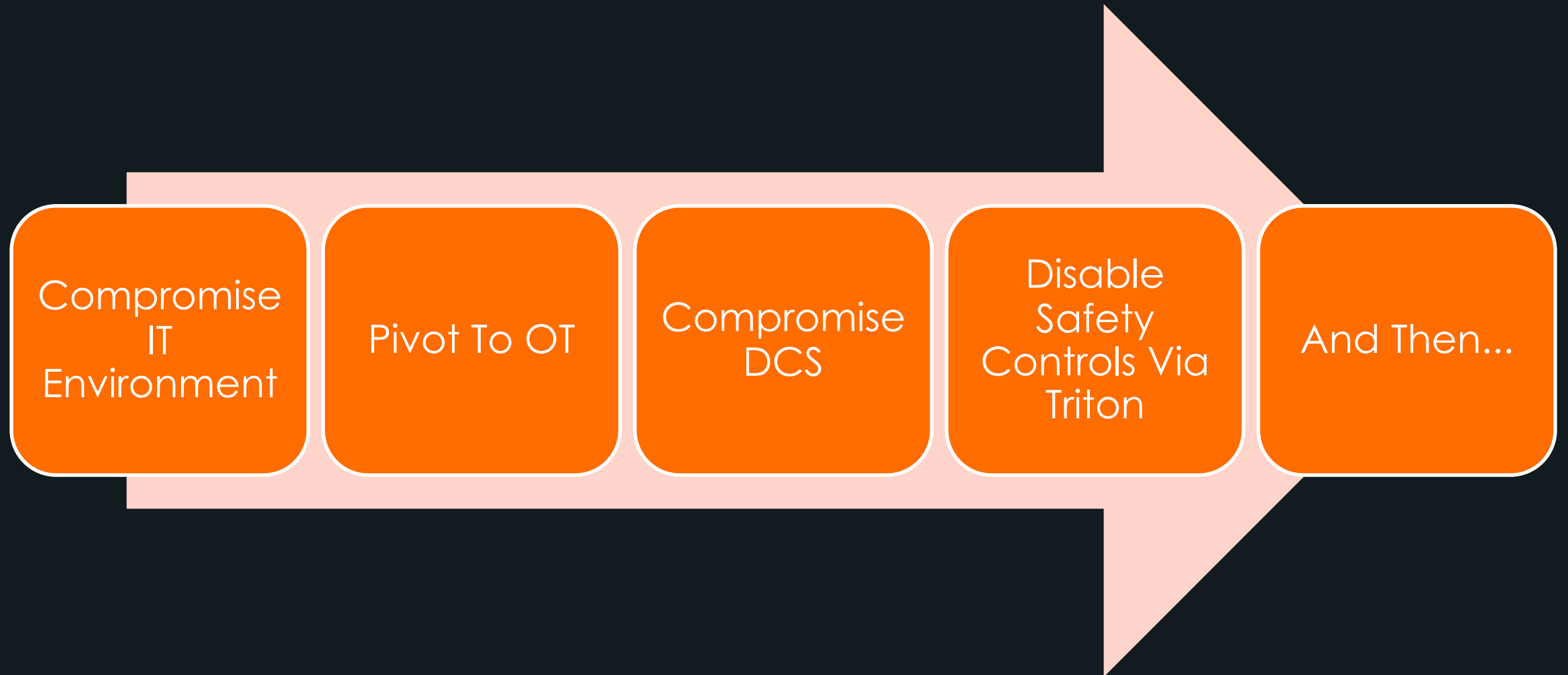
### MAR-17-352-01 HatMan—Safety System Targeted Malware

The HatMan malware affects Triconex controllers by modifying in-memory firmware to add additional programming. The extra functionality allows an attacker to read/modify memory contents and execute custom code on demand through receiving specially crafted network packets. HatMan consists of two pieces: a PC-based component to communicate with the safety controller and a malicious binary component that is downloaded to the controller. Safety controllers are used in a large number of environments, and the capacity to disable, inhibit, or modify the ability of a process to fail safely can potentially result in physical consequences. This malware analysis report discusses the components and capabilities of the HatMan malware and some potential mitigations. Media reporting also refers to this malware as both TRITON and TRISIS. This report is available at: [MAR-17-352-01 HatMan—Safety System Targeted Malware](#).

---

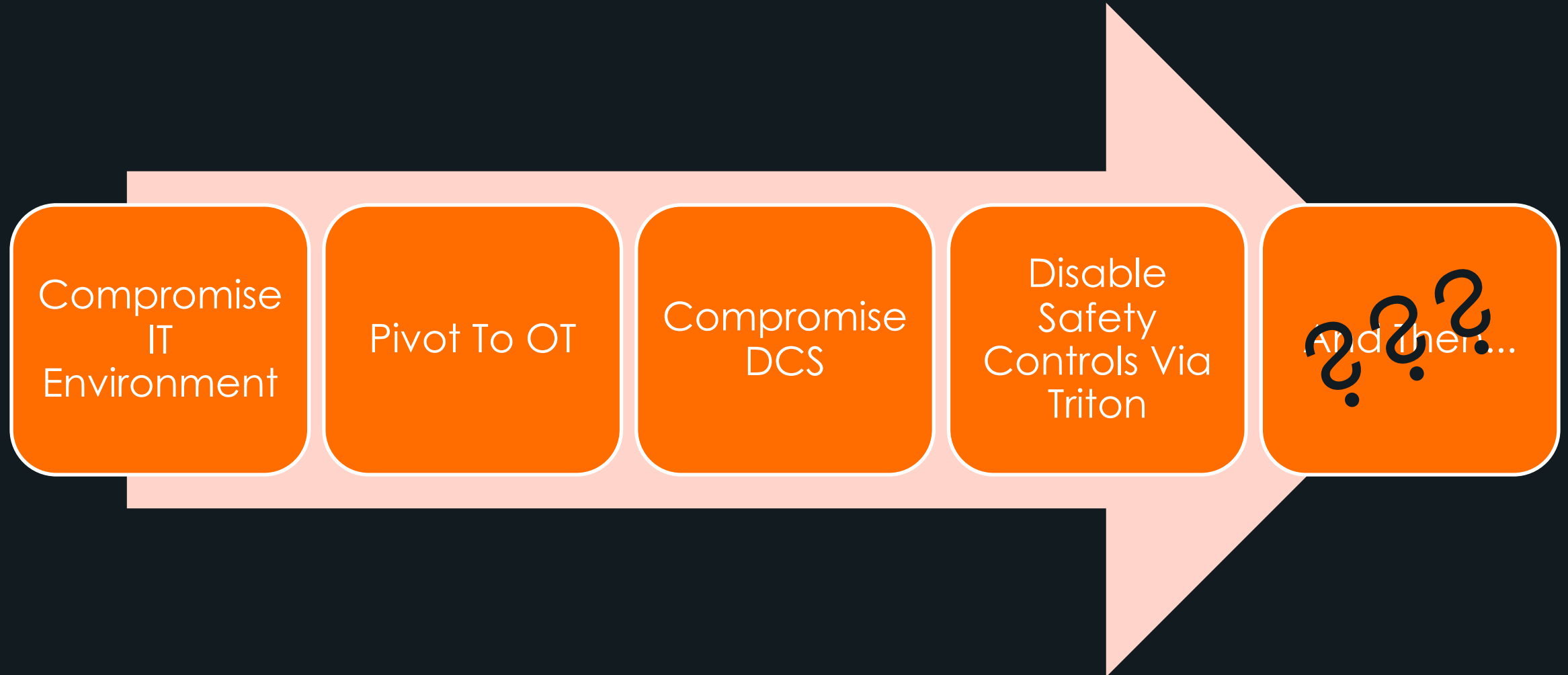
# Triton Attack Path

The Triton Event



# Triton Attack Path

The Triton Event



Compromise  
IT  
Environment

Pivot To OT

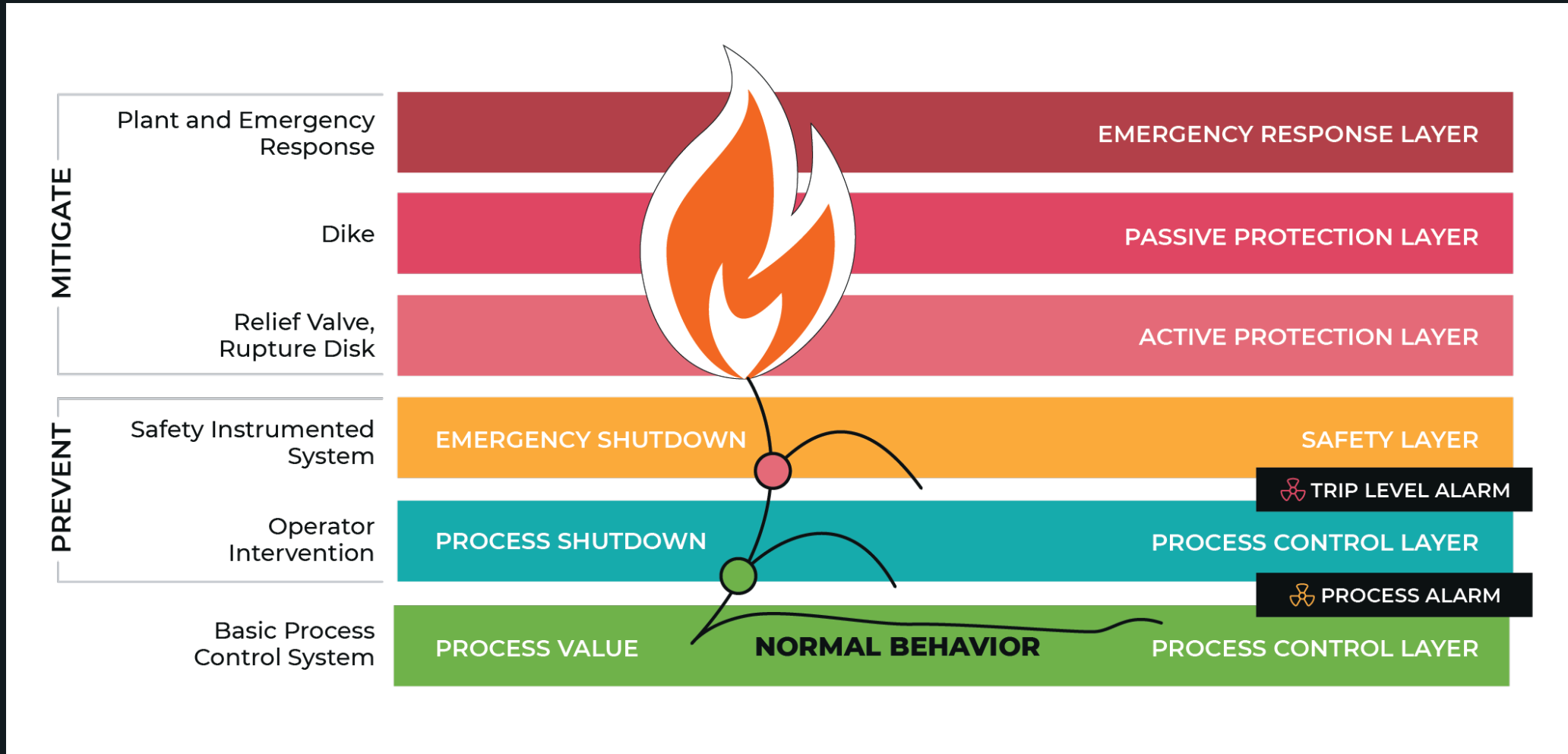
Compromise  
DCS

Disable  
Safety  
Controls Via  
Triton

And then...  
???

# Triton And Safety-Instrumented Systems

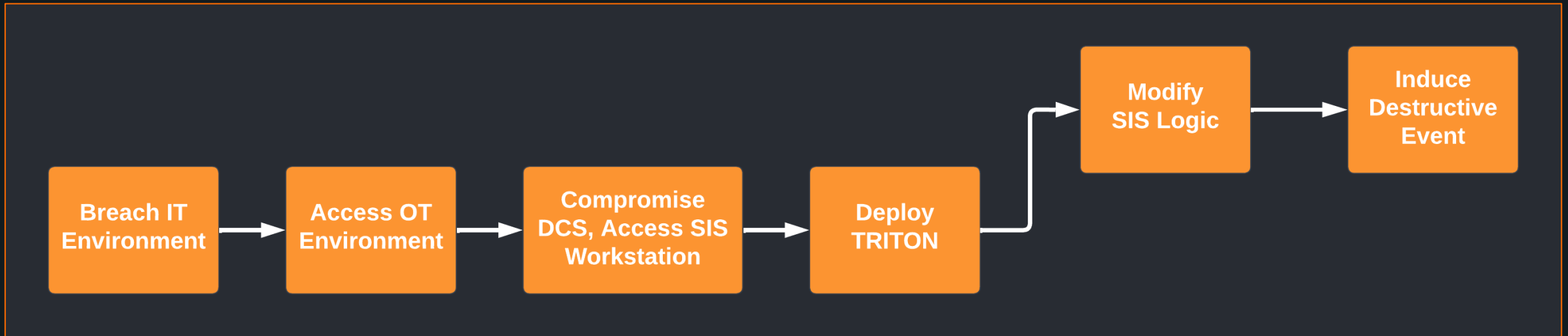
The Triton Event





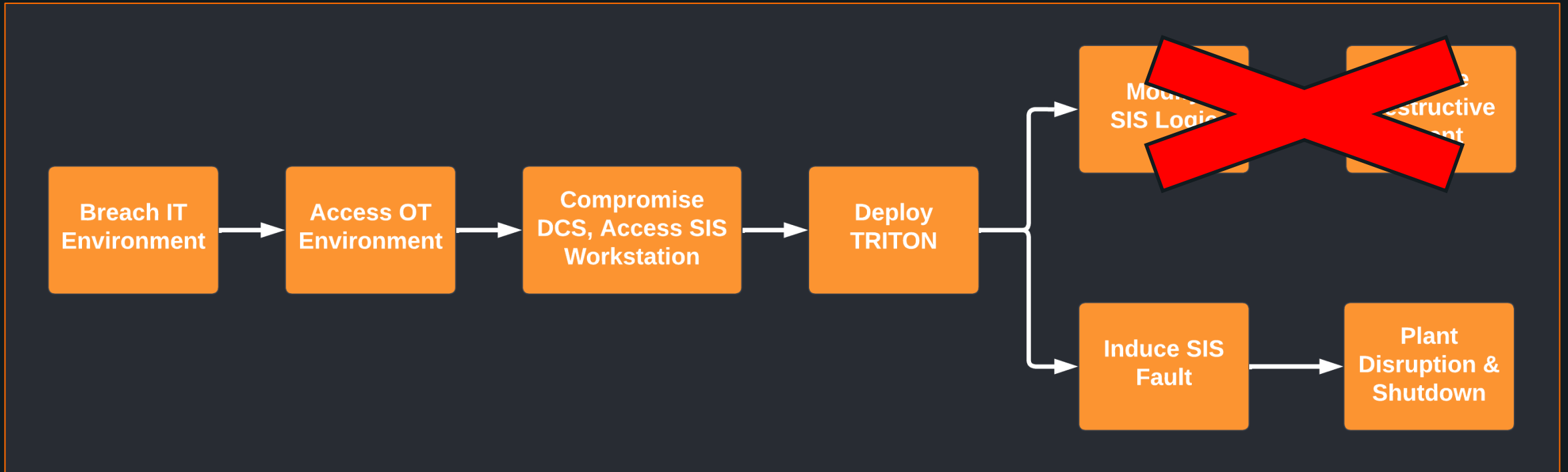
# Triton Intention?

The Triton Event



# Triton Result

The Triton Event



# Triton Responsibility

The Triton Event

The screenshot shows a web page with a dark blue header containing the Mandiant logo and navigation links: Platform, Solutions, Intelligence, Services, Resources, and Company. The main content area is white and features the following text:

THREAT RESEARCH

## TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers

FIREEYE INTELLIGENCE

OCT 23, 2018 | 7 MINS READ

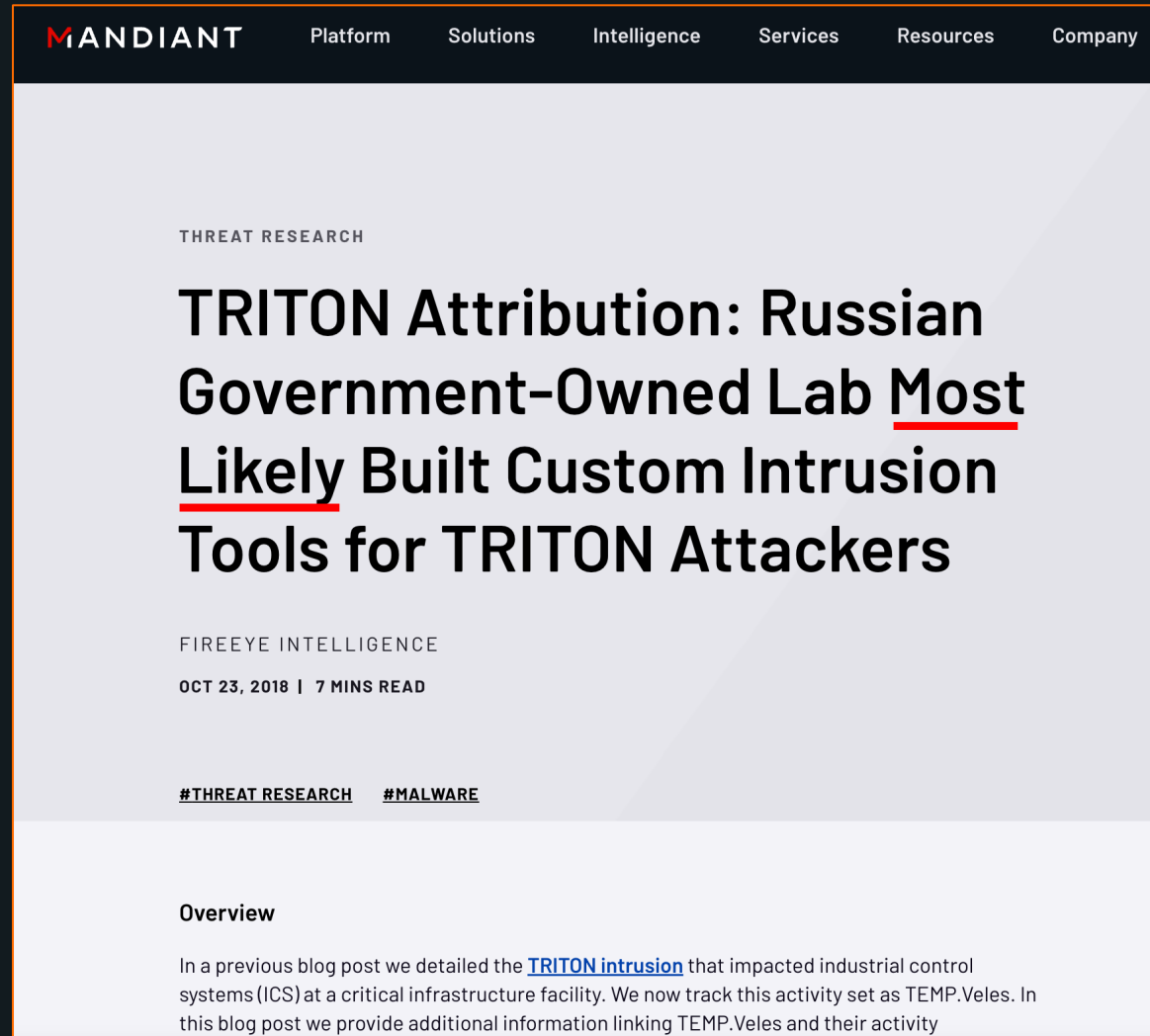
[#THREAT RESEARCH](#) [#MALWARE](#)

### Overview

In a previous blog post we detailed the [TRITON intrusion](#) that impacted industrial control systems (ICS) at a critical infrastructure facility. We now track this activity set as TEMP.Veles. In this blog post we provide additional information linking TEMP.Veles and their activity

# Triton Responsibility?

The Triton Event



The screenshot shows a web page with a dark blue header containing the Mandiant logo and navigation links: Platform, Solutions, Intelligence, Services, Resources, and Company. The main content area is white and features the following text:

THREAT RESEARCH

## TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers

FIREEYE INTELLIGENCE

OCT 23, 2018 | 7 MINS READ

[#THREAT RESEARCH](#) [#MALWARE](#)

### Overview

In a previous blog post we detailed the [TRITON intrusion](#) that impacted industrial control systems (ICS) at a critical infrastructure facility. We now track this activity set as TEMP.Veles. In this blog post we provide additional information linking TEMP.Veles and their activity

---

# Triton-Related Cryptonyms

The Triton Event

XENOTIME

Temp. Veles

???

# Follow-Up Actions

XENOTIME Post-Triton

**MANDIANT** Platform Solutions Intelligence Services Resources

THREAT RESEARCH

## TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping

STEVE MILLER, NATHAN BRUBAKER, DANIEL KAPELLMANN ZAFRA, DAN CABAN

APR 10, 2019 | 14 MINS READ

[#TTPS](#) [#THREAT RESEARCH](#) [#MALWARE](#)

### Overview

FireEye can now confirm that we have uncovered and are responding to **an additional intrusion by the attacker behind TRITON at a different critical infrastructure facility.**

**DRAGO** 

## Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas

 By Dragos, Inc. 06.14.19



**XENOTIME**

**CAPABILITIES**  
TRISIS, custom credential harvesting, off the shelf tools

**VICTIMOLOGY**  
Oil & Gas, Electric, Middle East, US, Europe, APAC

    The most dangerous threat to ICS has new targets in its sights. Dragos identified the XENOTIME activity group expanded its targeting beyond oil and gas to the electric utility sector. This expansion to a new vertical illustrates a trend that will likely continue for other ICS-targeting adversaries.

# US Government Disclosure - OFAC

XENOTIME Post-Triton

The screenshot shows the U.S. Department of the Treasury website. The header includes the Treasury seal and the text "U.S. DEPARTMENT OF THE TREASURY". A navigation bar contains links for "ABOUT TREASURY", "POLICY ISSUES", "DATA", "SERVICES", and "NEWS". Below the navigation bar, there is a green banner with the text "We can do this. Find COVID-19 vaccines near you." The main content area is titled "NEWS" and "PRESS RELEASES". On the left side, there is a sidebar menu with links for "Press Releases", "Statements & Remarks", "Readouts", "Testimonies", "Featured Stories", "Webcasts", and "Press Contacts". The main article is titled "Treasury Sanctions Russian Government Research Institution Connected to Triton Malware". The date is "October 23, 2020". The text of the article begins with "Washington – Today, the Department of the Treasury’s Office Control (OFAC) designated, pursuant to Section 224 of the Co Adversaries Through Sanctions Act (CAATSA), a Russian government institution that is connected to the destructive Triton malware – known also as TRISIS and HatMan in open source reporting – was designed specifically to target and manipulate industrial safety systems. Such systems provide for the safe emergency shutdown of industrial processes at critical infrastructure facilities in order to protect human life. The cyber actors behind the

## Triton Malware

In August 2017, a petrochemical facility in the Middle East was the target of a cyber-attack involving the Triton malware. This cyber-attack was supported by the **State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM)**, a Russian government-controlled research institution that is responsible for building customized tools that enabled the attack.

The Triton malware was designed to target a specific industrial control system (ICS) controller used in some critical infrastructure facilities to initiate immediate shutdown procedures in the event of an emergency. The malware was initially deployed through phishing that targeted the petrochemical facility. Once the

# US Government Disclosure - OFAC

XENOTIME Post-Triton

The screenshot shows the U.S. Department of the Treasury website. The header includes the Treasury logo and the text "U.S. DEPARTMENT OF THE TREASURY". Below the header is a navigation bar with links for "ABOUT TREASURY", "POLICY ISSUES", "DATA", "SERVICES", and "NEWS". A green banner below the navigation bar contains the text "We can do this. Find COVID-19 vaccines near you." The main content area is titled "NEWS" and "PRESS RELEASES". On the left side, there is a sidebar menu with links for "Press Releases", "Statements & Remarks", "Readouts", "Testimonies", "Featured Stories", "Webcasts", and "Press Contacts". The main article is titled "Treasury Sanctions Russian Government Research Institution Connected to Triton Malware" and is dated "October 23, 2020". The article text begins with "Washington – Today, the Department of the Treasury’s Office Control (OFAC) designated, pursuant to Section 224 of the Co Adversaries Through Sanctions Act (CAATSA), a Russian government institution that is connected to the destructive Triton malware — known also as TRISIS and HatMan in open source reporting — was designed specifically to target and manipulate industrial safety systems. Such systems provide for the safe emergency shutdown of industrial processes at critical infrastructure facilities in order to protect human life. The cyber actors behind the

## Triton Malware

In August 2017, a petrochemical facility in the Middle East was the target of a cyber-attack involving the Triton malware. This cyber-attack was supported by the **State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (TsNIKhM)**, a Russian government-controlled research institution that is responsible for building customized tools that enabled the attack.

The Triton malware was designed to target a specific industrial control system (ICS) controller used in some critical infrastructure facilities to initiate immediate shutdown procedures in the event of an emergency. The malware was initially deployed through phishing that targeted the petrochemical facility. Once the



# US Government Disclosure – Indictment

XENOTIME Post-Triton

FOR IMMEDIATE RELEASE

Thursday, March 24, 2022

## **Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide**

### **Defendants' Separate Campaigns Both Targeted Software and Hardware for Operational Technology Systems**

The Department of Justice unsealed two indictments today charging four defendants, all Russian nationals who worked for the Russian government, with attempting, supporting and conducting computer intrusions that together, in two separate conspiracies, targeted the global energy sector between 2012 and 2018. In total, these hacking campaigns targeted thousands of computers, at hundreds of companies and organizations, in approximately 135 countries.

A June 2021 indictment returned in the District of Columbia, *United States v. Evgeny Viktorovich Gladkikh*, concerns the alleged efforts of an employee of a Russian Ministry of Defense research institute and his co-conspirators to damage critical infrastructure outside the United States, thereby causing two separate emergency shutdowns at a foreign targeted facility. The conspiracy subsequently attempted to hack the computers of a U.S. company that managed similar critical infrastructure entities in the United States.

4. As set forth in greater detail below, GLADKIKH and co-conspirators known and unknown to the Grand Jury, including TsNIIKhM and members of TsNIIKhM and ADC, prepared, supported, conducted, and conspired to conduct computer intrusions using ADC resources that targeted energy facilities in the United States and elsewhere. Between in or around May and September 2017, they gained unauthorized access to the systems of a refinery outside the United

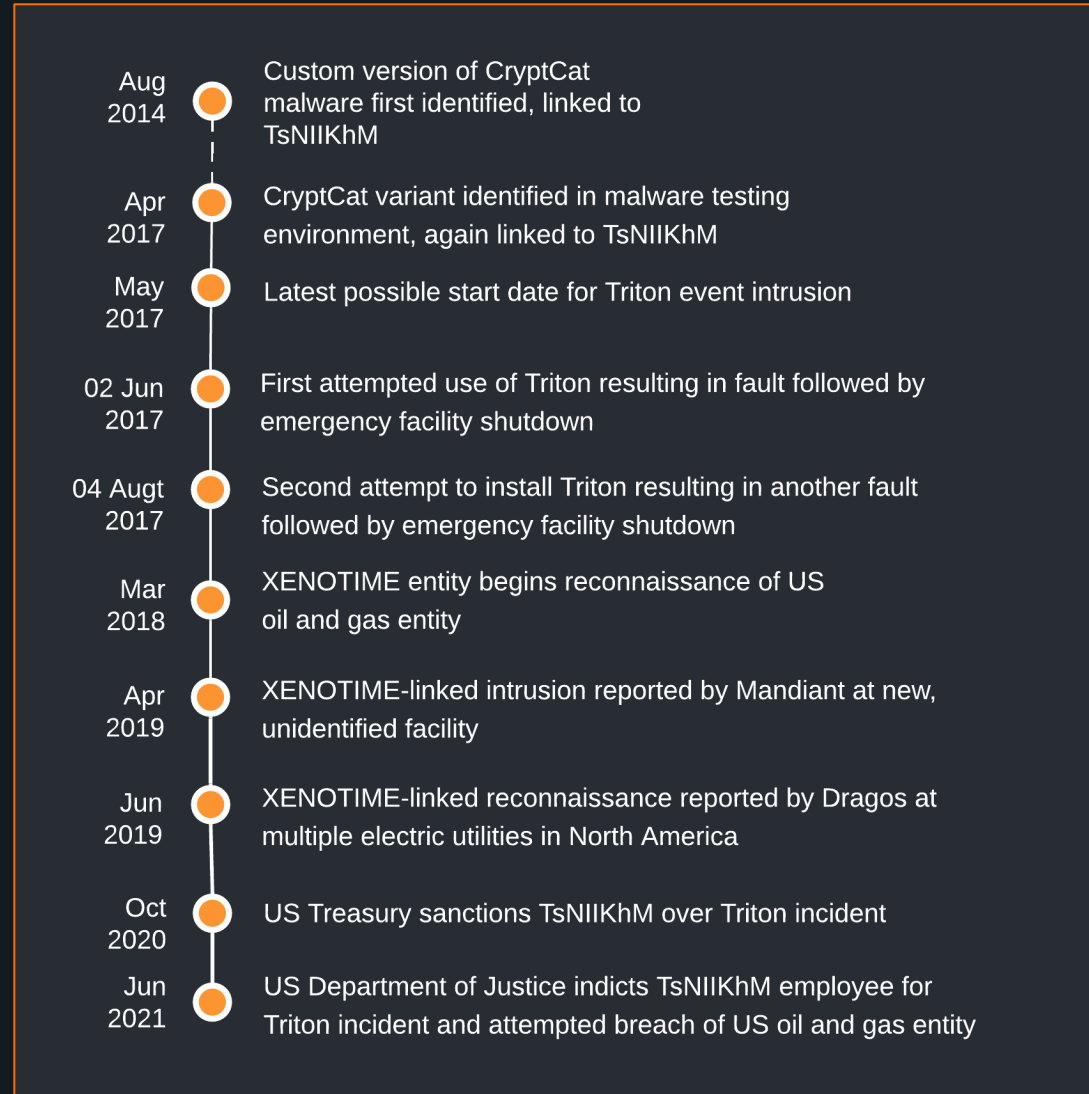
2

Case 1:21-cr-00442-CJN Document 1 Filed 06/29/21 Page 3 of 17

States using techniques and tools designed to enable an attacker to cause effects including physical damage, with potentially catastrophic effects, rather than merely causing a plant shutdown. In so doing they triggered an emergency shutdown of that facility's operations. Then, between in or around February and July 2018, GLADKIKH and co-conspirators targeted a U.S.-based company's similar facilities with similar techniques and tools and attempted to gain unauthorized access to its systems. Those 2018 attempts were unsuccessful.

# Overview Of Events

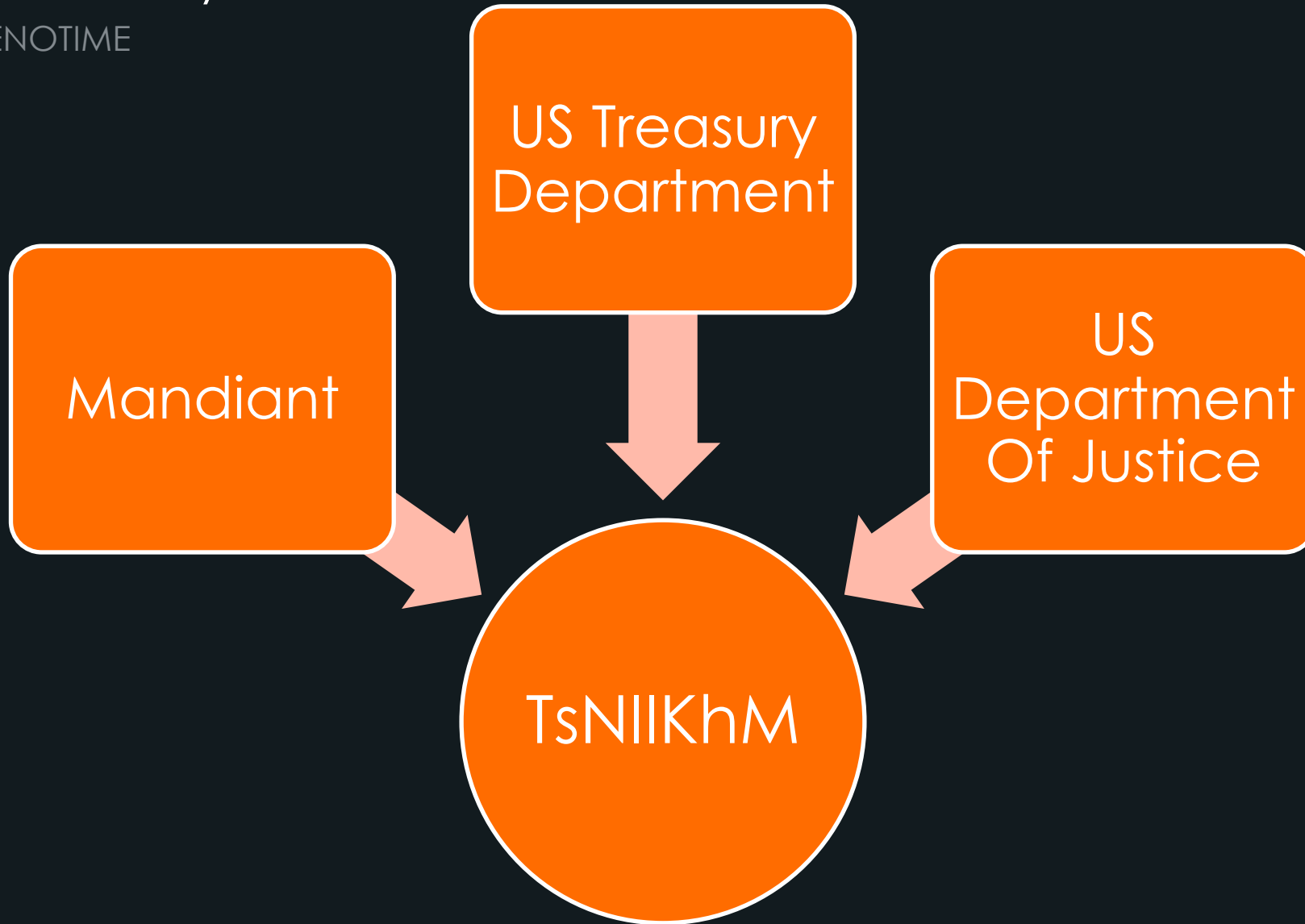
## XENOTIME Post-Triton



---

# Identifying An Entity

TsNIIKhM and XENOTIME



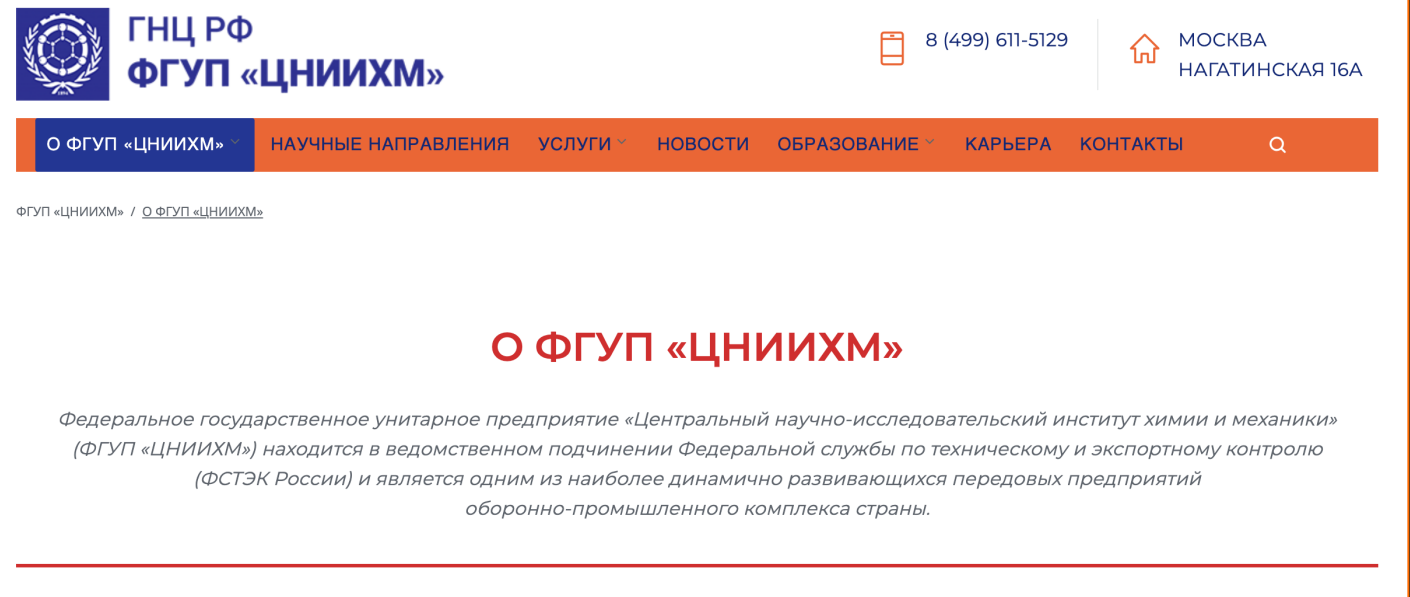
# What Is TsNIIKhM???

TsNIIKhM and XENOTIME



<https://www.thespacereview.com/archive/3709b.jpg>

<https://www.thespacereview.com/archive/3709a.jpg>



ГНЦ РФ  
ФГУП «ЦНИИХМ»

8 (499) 611-5129

МОСКВА  
НАГАТИНСКАЯ 16А

О ФГУП «ЦНИИХМ» НАУЧНЫЕ НАПРАВЛЕНИЯ УСЛУГИ НОВОСТИ ОБРАЗОВАНИЕ КАРЬЕРА КОНТАКТЫ

ФГУП «ЦНИИХМ» / О ФГУП «ЦНИИХМ»

## О ФГУП «ЦНИИХМ»

Федеральное государственное унитарное предприятие «Центральный научно-исследовательский институт химии и механики» (ФГУП «ЦНИИХМ») находится в ведомственном подчинении Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и является одним из наиболее динамично развивающихся передовых предприятий оборонно-промышленного комплекса страны.

---

# TsNIIKhM Operations

TsNIIKhM and XENOTIME

Explosives  
Research

Space  
Weapons

Autonomous  
Vehicles

Cyber  
Research

Advanced  
Chemistry

'The Federal State Unitary Enterprise "Central Research Institute of Chemistry and Mechanics" (FGUP "TsNIIKhM") is subordinated to the Federal Service for Technical and Export Control (FSTEC of Russia) and is one of the most dynamically developing advanced enterprises of the country's military-industrial complex.'

# TsNIIKhM & ADC

TsNIIKhM and XENOTIME

Государственный научный центр Российской Федерации  
Федеральное государственное унитарное предприятие

«Центральный научно-исследовательский институт химии и механики»

8(499)611-51-29 8(499)782-23-21ф

ОБРАТНАЯ СВЯЗЬ

О предприятии ГНЦ РФ Карьера Услуги Социальная сфера Контакты Фотогалерея

Главная >> О предприятии >> Направление деятельности >> Центр прикладных разработок

[О предприятии](#)

[Руководство](#)

[Направление деятельности](#)

- [Научно-исследовательский центр нанотехнологий](#)
- [Конструкторское бюро](#)

## Центр прикладных разработок

Проведение поисковых и прикладных исследований по обоснованию и созданию средств и методов защиты критически важных объектов инфраструктур Российской Федерации от деструктивного воздействия информационного и технологического характера.

‘Conducting exploratory and applied research to substantiate and create means and methods for protecting critically important infrastructure facilities of the Russian Federation from the destructive impact of information and technological nature.’

# TsNIIKhM & ADC

TsNIIKhM and XENOTIME

Государственный научный центр Российской Федерации  
Федеральное государственное унитарное предприятие

«Центральный научно-исследовательский институт химии и механики»

8(499)611-51-29 8(499)620-3-21ф

ОБРАТНАЯ СВЯЗЬ

О предприятии ГНЦ РФ Карьера Услуги Социальная сфера Контакты Фотогалерея

Главная >> О предприятии >> Направление деятельности >> Центр прикладных разработок

## Центр прикладных разработок

Проведение поисковых и прикладных исследований по обоснованию и созданию средств и методов защиты критически важных объектов инфраструктуры Российской Федерации от деструктивного воздействия информационно-технологического характера.

[О предприятии](#)

[Руководство](#)

[Направление деятельности](#)

- [Научно-исследовательский центр нанотехнологий](#)
- [Конструкторское бюро](#)

‘Conducting exploratory and applied research to substantiate and create means and methods for protecting critically important infrastructure facilities of the Russian Federation from the destructive impact of information and technological nature.’

---

# TsNIKhM Role?

TsNIKhM and XENOTIME





# TsNIKhM Role?

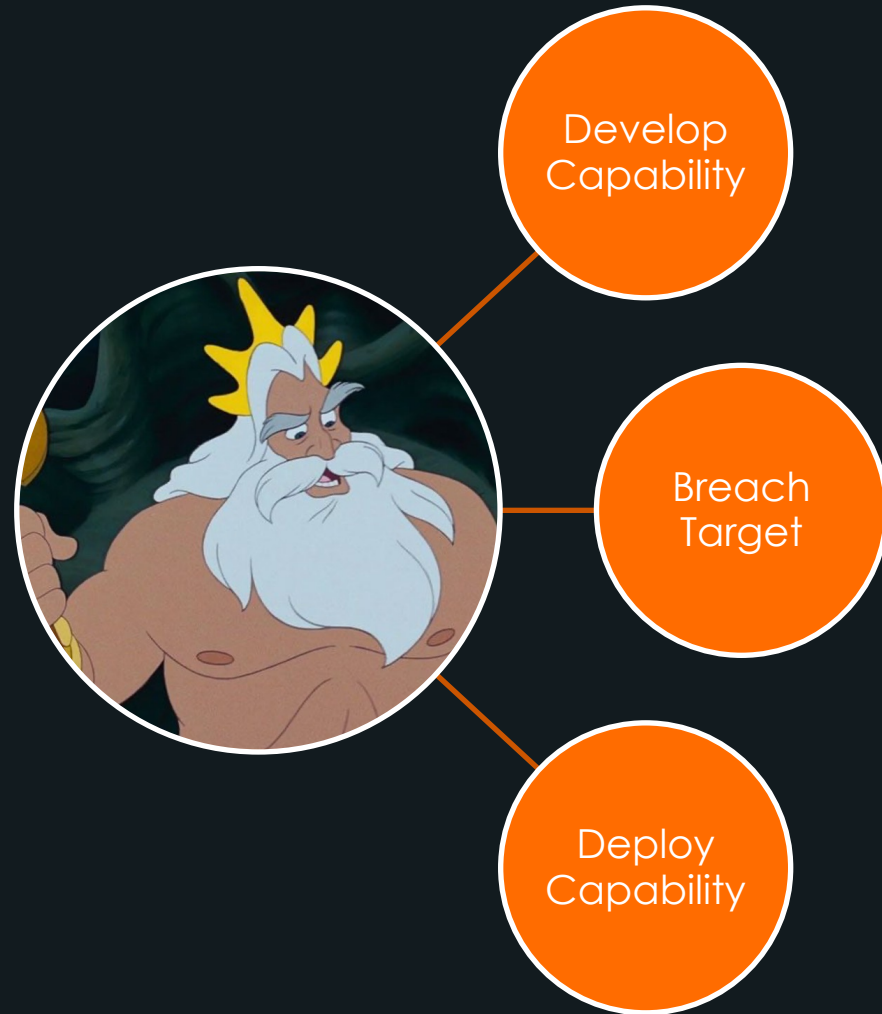
TsNIKhM and XENOTIME



---

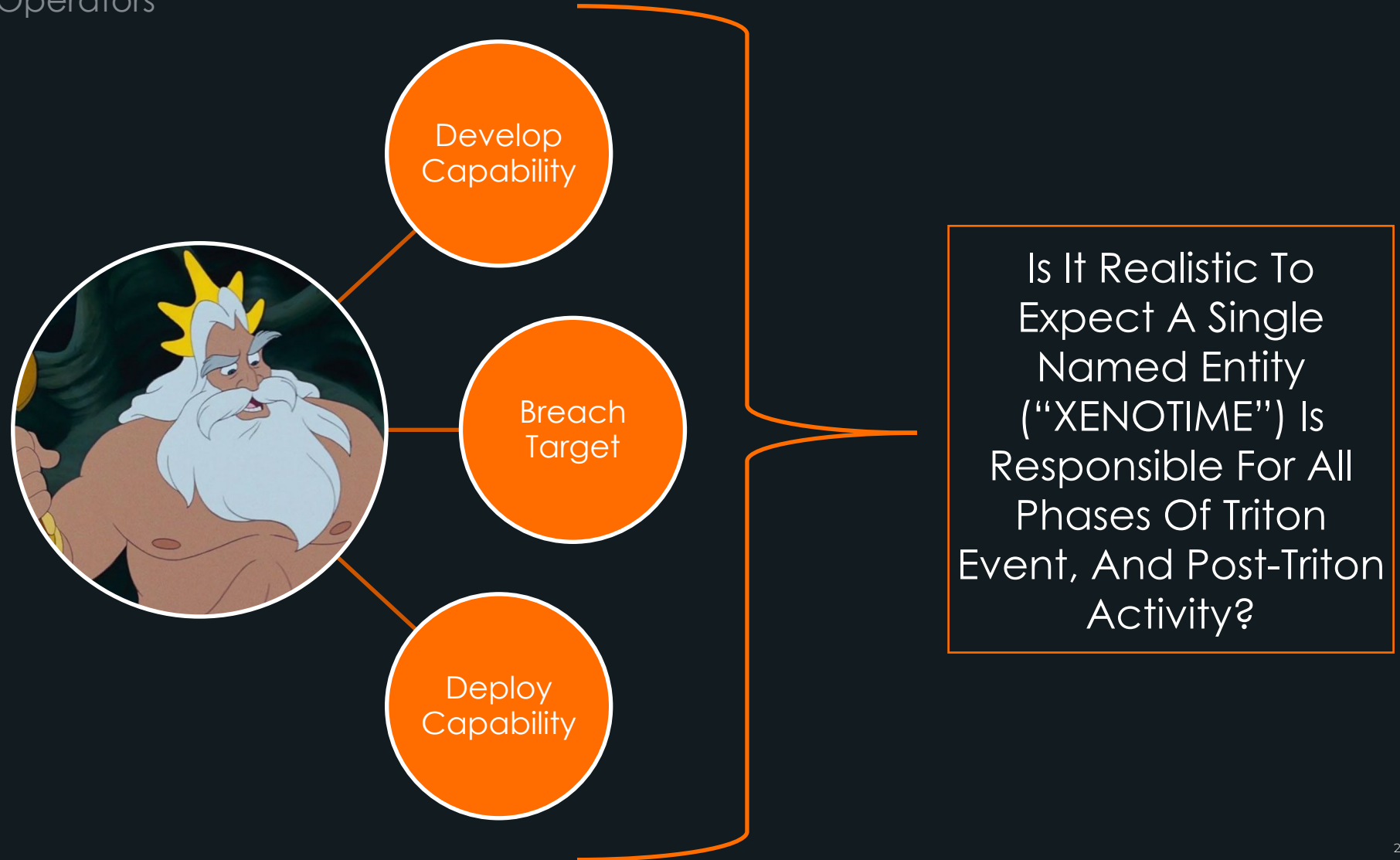
# Triton & XENOTIME

Developers, Actors, & Operators



# Triton & XENOTIME

Developers, Actors, & Operators



# Unearthing An Ecosystem

Developers, Actors, & Operators

Ministry of Defence of the Russian Federation  
Era military innovative technopolis

ARMY 2020    MULTIMEDIA    CONTACTS    HOW TO GET TO

0 : 00 : 00 : 00  
дней    часов    минут    секунд

Events

- Static Exposition
- Demonstration Programme
- Business Programme

Speech by Minister of Defence Sergei Shoigu

Speech by Deputy Defence Minister Pavel Popov

Reports

КВАНТ  
Федеральное государственное унитарное предприятие научно-исследовательский институт "Квант"

Главная    Новости    Закупки    Образование и наука    Работа    Контакты

Поиск

### ФГУП «НИИ «Квант»

Федеральное государственное унитарное предприятие «Научно-исследовательский институт «Квант» (ФГУП «НИИ «Квант»), основанное на праве хозяйственного ведения, создано в январе 1978 года.

ФГУП «НИИ «Квант» является коммерческим юридическим лицом, созданным для удовлетворения государственных и общественных потребностей в области создания специальных технических и программных средств. Основными видами деятельности института являются:

- проведение фундаментальных, поисковых и прикладных научных исследований, научно-исследовательских и опытно-конструкторских работ в области создания электронно-вычислительной техники, техники связи и телекоммуникаций, систем и средств обработки данных и изделий радиоэлектронной и вычислительной техники;
- разработка, производство, реализация, ремонт, гарантийное и послегарантийное обслуживание электронно-вычислительных средств и комплексов специального и гражданского назначения, в том числе

НАВИГАЦИЯ

Новости

О предприятии

Направление деятельности

Руководство

Наша история

Специальная оценка условий труда

Закупки

Положение о закупках

Документация

План закупок

Информация

Образование и наука

Совет молодых специалистов

Работа

Профсоюз

Контакты

НОВОСТИ

ОСТОРОЖНО – МОШЕННИКИ!

Поздравление с 8 Марта

Поздравление с Новым Годом

Home    For Media    Contact us

MOD | SFLMRD    MILITARY SCIENTIFIC COMMITTEE    SCIENTIFIC RESEARCH

Peacekeeping operations

All exercises

Peacekeeping operations

Sociological center

International Mine Action Center

The 24th Central Research branch of the Military Academy named after a Kuznetsov

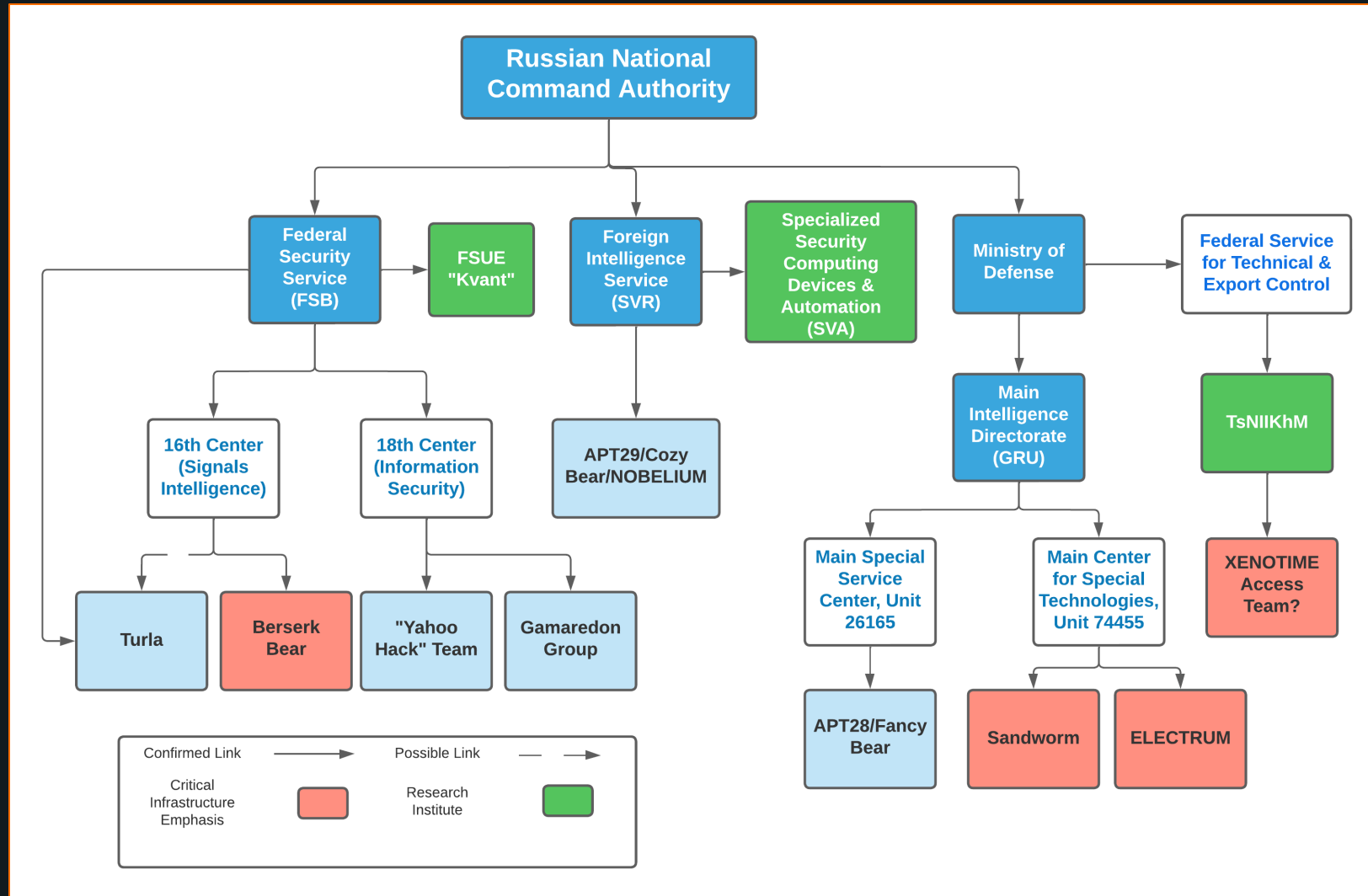
The 40th State Research Institute of the Ministry of Defence of the Russian Federation - branch of the Military Educational-and-Research Centre Naval Academy named after Admiral of the Fleet of the Soviet Union N.G. Kuznetsov

The 25th State Research Institute of chemmology of the Ministry of Defence of the Russian Federation

The 27th Central Research Institute of the Ministry of Defence of the Russian Federation

# Unearthing An Ecosystem

Developers, Actors, & Operators



---

# Triton, Revisited

Developers, Actors, & Operators

Cyber Operations - Especially Targeted Events - Are Extremely Complex!



Division Of Labor Among Various Parties To Achieve Outcomes



One "Actor" Is Rarely Responsible For Everything

---

# Triton, Revisited

Developers, Actors, & Operators

We Can Assess With High Confidence That The Triton Incident Represents A Collaborative Action Among Multiple Parties (Many Unknown At This Time, But Likely Linked To Russian Military Intelligence) Across Tasking, Development, And Intrusion Actions.

---

# So What Is "XENOTIME???"

Developers, Actors, & Operators



"XENOTIME" Is A Composite Of Multiple Entities

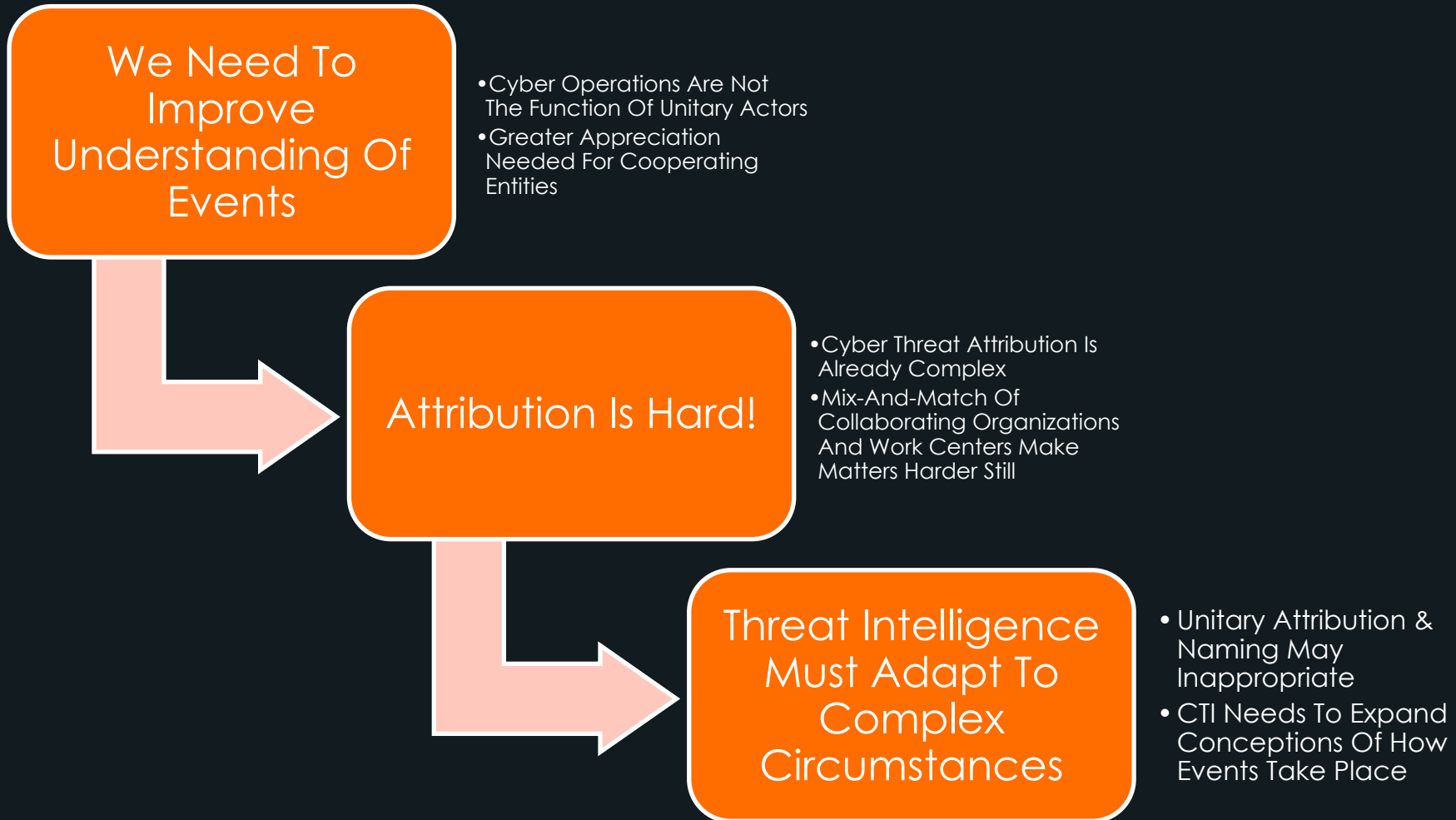
Range Of Actions Indicate Complex Interaction  
Between Organizations

We Still Do Not Know Critical Elements Of XENOTIME  
Activity



# Why Does This Matter?

Developers, Actors, & Operators



---

# Thank you

[Joe.slowik@gigamon.com](mailto:Joe.slowik@gigamon.com)

[@jfslowik](https://twitter.com/jfslowik)

---

# References

## Selected Items

- Sobczak, B. The Inside Story of the World's Most Dangerous Malware. E&E News. 07 March 2019. <https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/>
- Gutmanis, J. Triton – A Report from the Trenches. YouTube. 11 March 2019. <https://www.youtube.com/watch?v=XwSJ8hloGvY>
- Johnson, B.; Caban, D.; Krotofil, M.; Scali, D.; Brubaker, N.; Glycer, C. Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure. Mandiant. 14 December 2017. <https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton>
- Dragos. TRISIS Malware: Analysis of Safety System Targeted Malware. 13 December 2017. <https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf>
- FireEye Intelligence. TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. 23 December 2018. <https://www.mandiant.com/resources/triton-attribution-russian-government-owned-lab-most-likely-built-tools>
- US Department of the Treasury. Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware. 23 October 2020. <https://home.treasury.gov/news/press-releases/sm1162>.
- Slowik, J. The Past and Future of Integrity-Based Attacks in ICS. Dragos. <https://www.dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf>
- Miller, S., Brubaker, N.; Kapellmann Zafra, D.; Caban, D. TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping. Mandiant. 10 April 2019. <https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections>
- Wightman, R.; Wylie, J. Analyzing TRISIS. Vimeo. 2018. <https://vimeo.com/275906105>.
- US Department of Justice. Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide. 24 March 2022. <https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical>
- US Department of Justice. United States of America v. Evgeny Viktorovich Gladkikh. 25 May 2021. <https://www.justice.gov/opa/press-release/file/1486831/download>