28 - 30 September, 2022 / Prague, Czech Republic

ZEROING IN ON XENOTIME: ANALYSIS OF THE ENTITIES RESPONSIBLE FOR THE TRITON EVENT

Joe Slowik

Gigamon, USA

joe.slowik@gigamon.com

ABSTRACT

The 2017 Triton or TRISIS event targeted safety systems at an oil and gas processing facility in Saudi Arabia. Although all available evidence indicates the attack likely failed in its overall execution, the incident stands out as the first attempted cyber event that contained the possibility for direct harm or loss of life. While gathering headlines for some months after the incident was publicly revealed in late 2017, further reporting on the actor responsible – referred to as XENOTIME – appeared to dry up, leaving many unanswered questions.

Matters changed in 2022 with a combination of some very broad industry reporting and the public release of a US Department of Justice indictment from 2021 identifying a specific persona behind the Triton incident. While adding some context around the group, many questions remain unanswered, not the least of which being what this entity (or its component organizations) has been up to since 2017.

This presentation will delve deeper into the specific entity (or perhaps more plausibly, entities?) responsible for the 2017 event, and the implications of this association. While earlier reporting identified a specific research institution as linked to the 2017 incident, an observation seemingly reinforced by the indictment, further analysis reveals that this entity likely served primarily tool development, testing and research functions, leaving the actual perpetrators unidentified beyond loose country association. By exploring technical, targeting and geopolitical factors surrounding the events in Saudi Arabia, as well as discussing additional activity linked to this actor between 2018 and 2022, we will gain greater understanding of just who XENOTIME might be and its implications for overall critical infrastructure cyber operations since the Triton event.

INTRODUCTION

In 2017, a petrochemical facility in Saudi Arabia experienced multiple, unexpected, and (initially) unexplained shutdowns [1]. Taking place in June and again in August 2017, multiple Safety Instrumented Systems (SIS), also referred to as Emergency Shutdown Devices (ESD), inexplicably tripped, inducing disruption in the industrial environment [2]. Subsequent investigation of the August incident revealed several interesting artifacts residing on a safety system workstation, most notably a framework for surreptitiously interacting with *Schneider Electric Triconex* SIS devices – ultimately given the name Triton [3].

Also referred to as TRISIS and HatMan, [4, 5] analysis indicated Triton was designed to enable an attacker to arbitrarily – and silently – modify a *Triconex* SIS, enabling potentially catastrophic, and even deadly, outcomes. Yet initial reporting provided little, if any, detail as to what entity was responsible for the incident in question. Further research (as well as actions from the US government) linked Triton to a research institute in Russia, the State Research Center of the Russian Federation Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) [6, 7].

Although undeniably linked to events in 2017, TsNIIKhM is an odd organization to engage in operations described by some as 'malware that can kill' [8]. More significantly, aside from limited leaks and government actions, in five years no further substantial events have specifically been identified and irrefutably linked to the adversary responsible for Triton, referred to in commercial reporting as XENOTIME [9]. In this paper we will review the 2017 Triton incident, discuss follow-on operations associated with the group responsible, and then explore what 'XENOTIME' plausibly means. Through this examination, we will study the differentiation between developers and actors in cyber operations, and what this means for incidents where visibility is limited, and multiple parties are likely at play.

THE TRITON INCIDENT

Based on multiple public disclosures, the Triton incident targeted the Petro Rabigh joint venture petrochemical facility in Saudi Arabia [1]. Interestingly, the plant disruptions took place several times, resulting in facility shutdowns – but not something more catastrophic given that SIS devices were the attacker's final targets. Based on the capability deployed (a multi-part framework to quietly and arbitrarily modify safety logic in industrial environments) and the effects achieved (plant shutdown), a disconnect seems to exist as the latter effect could be more easily attained via other, more direct means.

As analysed previously [10], Triton likely represents an ambitious attempt to create a cyber-physical impact that ultimately failed for reasons still not completely understood. Based upon public analysis and disclosure, XENOTIME thoroughly compromised the victim environment, from initial IT breach and lateral movement [11], through entry into the Distributed Control System (DCS) network and finally the safety network [1, 2]. Mechanisms used to facilitate this vary, from custom-developed tooling unique to XENOTIME to variations of several public frameworks to achieve persistence [11].

Irrespective of specific methodology, the intrusion appears focused on ultimately modifying environment safety logic to enable a physically destructive event, given the focus on safety controllers. While arbitrary modifications to the plant's DCS environment could prove disruptive, safety- and engineering-based mitigations, illustrated in Figure 1, can mitigate or eliminate worst-case scenarios for physical process impacts and destruction.

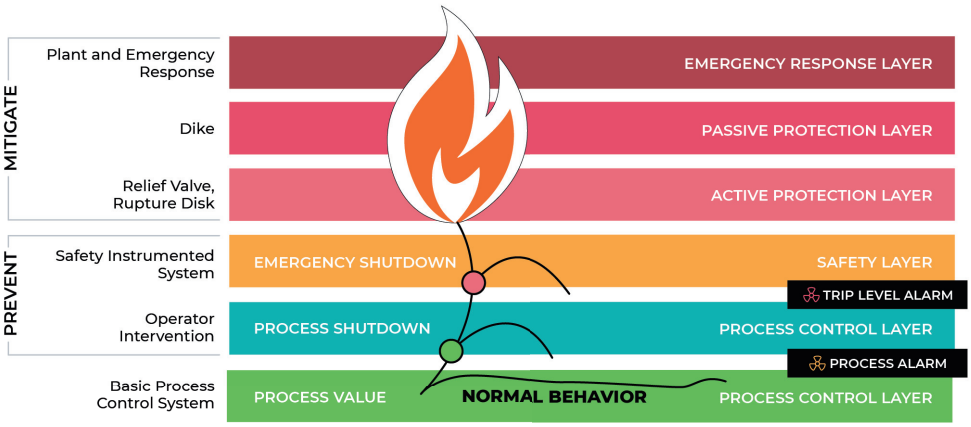

Figure 1: Safety and engineering controls in industrial environments.

An adversary that desires an effective physical impact would need to eliminate or otherwise disable SIS and related systems for a DCS modification to propagate to the physical environment and cause an impact. Reviewing the Triton incident considering these details, the most likely scenario pursued by XENOTIME was a dual-track intrusion: compromise and modification of facility SIS, to allow for subsequent modifications or disruptions in the plant's DCS to propagate through the safety layer to induce a physical impact. While engineering controls still exist beyond SIS devices, these nonetheless result in potentially dangerous outcomes such as emergency venting of product or triggering relief mechanisms.

Overall, Triton represents only a part of a broader, ambitious sequence of actions to produce a cyber-physical impact scenario. Outlined in Figure 2, XENOTIME planned and executed multiple actions across several distinct network segments before reaching a point where Triton itself could be deployed.

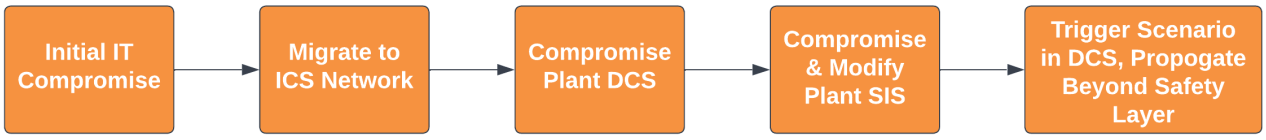

Figure 2: Triton attack stages and actions.

And yet, for all this complexity, the intrusion arguably failed in achieving the likely objective as described above. Rather than allowing XENOTIME to modify logic on the *Triconex* devices, Triton instead caused these devices to trigger a plant shutdown. While disruptive (and expensive), this scenario pales in comparison to the much more frightening possibility of an incident resulting in facility damage or even potential injury or death to on-site personnel.

While the precise reasons for Triton's failure are unknown, public analysis indicates a potential mismatch between the *Triconex* hardware and firmware combination used in the victim facility and the platform against which Triton was built [12]. Another, more likely explanation is a post-exploitation action immediately after Triton execution that triggered the controller crash [12, 13], although analysis from *Mandiant* and others failed to identify such a payload during post-incident investigation. Irrespective of why Triton largely failed, the framework triggered an immediate disruption of plant operations instead of the more nefarious action of enabling arbitrary modification to safety logic and other SIS functionality to induce a cyber-physical impact scenario.

We therefore see something of a paradox: an adversary patient enough to conduct a prolonged, multi-stage intrusion, capable of developing and deploying a malware framework with very specific (and alarming) functionality, but somehow incapable of correctly developing or executing this capability for the victim environment. XENOTIME presents itself as a conundrum – one that we will now analyse in greater detail.

IDENTIFYING AN ENTITY

Approximately one year after the public disclosure of Triton, researchers from *Mandiant* identified and detailed links between the intrusion and Russia-based TsNIIKhM. Specifically, several enabling tools identified in the victim environment were observed in an unspecified malware testing environment linked to a persona *Mandiant* linked to TsNIIKhM based on open-source research [6]. Additional observations, such as file metadata, correlating time of activity to standard working hours in Russia, and a possible username identified in observations potentially linked to a likely TsNIIKhM employee,

suggested at minimum links to a Russian entity. Overall, while a case could be made linking Triton (and potentially XENOTIME) to TsNIIKhM, initial evidence (where presented) appeared largely circumstantial and incomplete at this time.

Matters changed significantly in 2020, when the US Department of the Treasury's (USDT) Office of Foreign Assets Control (OFAC) sanctioned TsNIIKhM, specifically for its involvement in enabling the Triton event [7]. While adding the weight of government confirmation to *Mandiant*'s prior analysis, the press release detailing sanctions noted responsibility 'for building customized tools that enabled [the Triton] attack'. A savvy reader will notice the Treasury statement does *not* assign responsibility for building Triton, or for using the malware in the victim environment, to TsNIIKhM. Instead, the USDT OFAC statement appears to mirror *Mandiant*'s findings, linking TsNIIKhM to enabling tools used during the Triton incident.

Further details emerged in March 2022, when a 2021 indictment from the US Department of Justice (DOJ), *United States v. Evgeny Viktorovich Gladkikh*, was publicly disclosed [14]. This indictment specifically identified a TsNIIKhM employee, Gladkikh, and unidentified co-conspirators as responsible for the actual operations leading to the deployment of Triton (as well as actions against an unspecified oil and gas entity in the United States, discussed in greater detail below). Again, responsibility for Triton's development is left unsaid. At this stage, TsNIIKhM's *association* with Triton and subsequent activities tracked as XENOTIME is well established, but specific details regarding event execution and responsibility remain fuzzy.

Looking at the institute in question more closely, TsNIIKhM was founded in 1894 initially for development and manufacture of smokeless powder for the Russian empire [15]. Since that time, the institute has diversified operations into a variety of fields while remaining linked to Russia's Ministry of Defence (MOD). As noted by both *Mandiant* and DOJ reporting, identified individuals linked to Triton are connected to a specific entity housed within TsNIIKhM: the Applied Development Center (ADC). ADC's (now offline) website notes roles in critical infrastructure protection including references to potential cyber operations [16], with DOJ emphasizing concurrent, non-public roles in offensive tool research and development [14]. Overall, TsNIIKhM's operations remain oriented toward supporting Russian security, military, and related interests, with ADC appearing to be a particularly sensitive entity within the organization.

TsNIIKhM presents itself as a logical entity to research, develop, and create a tool such as Triton given the organization's mission as a research institution and its history supporting Russian military endeavours. Operationally, one may look at the entity as similar to government-funded laboratories with strong military or intelligence connections elsewhere. Yet where matters become confusing are the distinctions between tool development, tool prepositioning, and final tool deployment. While TsNIIKhM appears a reasonable entity to satisfy the initial stages, having a research institute (even if under Russian MOD sponsorship) actually undertake the infiltration of Petro Rabigh (and other organizations) appears very odd. At first glance, DOJ's indictment appears only to blame TsNIIKhM (and ADC) for *deploying* Triton (via Gladkikh), leaving development (presumably a function aligned with ADC's mission) unmentioned and unattributed.

Yet specific language in the DOJ indictment leaves some room for interpretation: 'Gladkikh and co-conspirators known and unknown to the Grand Jury, including TsNIIKhM and members of TsNIIKhM and ADC.' [17]. While Gladkikh, specifically called out as an employee of TsNIIKhM working in ADC, is directly identified, other involved parties remain unnamed – not an unprecedented action, but odd for a specific 'name-and-shame' action from the US government. The implication here is that entities aside from Gladkikh are involved, and while operational matters may link directly to Gladkikh, developmental efforts could reside with other, unnamed parties that reside within the same organizations.

Furthermore, DOJ's 2021 indictment uses the word 'including', leaving open the possibility that other entities or organizations beyond TsNIIKhM were involved in the Triton event and subsequent activities. Several possibilities emerge here, from the Russian MOD (through various intelligence entities under Russian military intelligence, also referred to as the GRU) participating in operations to other, non-military but state intelligence-linked bodies contributing to intrusions (or delivering operational tasking to TsNIIKhM and ADC).

Adding detail to XENOTIME's involvement, the DOJ indictment presents a timeline of actions linked to Gladkikh and his co-conspirators that also is intriguing. Actions specifically attributed to the individual include:

- Initial access to the Triton victim's IT network.
- Research and exfiltration of data related to *Triconex* SIS operations in the victim environment.
- Deploying and executing the custom version of CryptCat initially flagged by *Mandiant* as a link to TsNIIKhM.
- Pivoting into the operational technology (OT) network at Petro Rabigh via a dual-homed data historian, then migrating from this system to an engineering workstation connected to the victim's safety network.
- Two specific attempts (02 June and 04 August 2017) to install variants of Triton on *Triconex* devices, resulting in faults then system shutdowns.

Notably absent from the above list of actions are the development and testing of Triton itself. While Gladkikh appears to be the primary entity responsible for the Triton *intrusion*, the actual development of the 'malware that can kill' is linked to some other, unidentified entity. Before examining this mystery, a review of subsequent operations linked to XENOTIME – and by association, TsNIIKhM – is in order.

OPERATIONS SINCE 2017

Since the Triton event, the entity at minimum linked to, if not responsible for, the incident – referred to as XENOTIME by *Dragos*, but also referred to as Temp.Veles by *FireEye* and *Mandiant* – has remained active. Four particular phases of XENOTIME operation stand out given their focus and potential intention.

First, shortly after the Triton event and as documented by DOJ, XENOTIME (and Gladkikh specifically) engaged in initial reconnaissance and access activity against a US-based oil and gas company [17]. Although resulting in no identified disruption, or recognized attempt at a physically destructive event such as in the Triton incident, DOJ reporting indicates significant, focused interest in critical aspects of US oil and gas infrastructure. Based on available information, at minimum Gladkikh, and overall XENOTIME activity, sought to preposition within US critical infrastructure in the oil and gas sector. While there are many potential reasons for doing so, such actions would be necessary precursors for enabling a future Triton-like scenario within the victim systems.

In parallel with the above, researchers at *Mandiant* revealed a second intrusion linked to XENOTIME. Reported in 2019, it is unclear when the intrusion took place, let alone the victim or even the industry in which the victim operates [11]. However, *Mandiant* reporting suggested that XENOTIME-linked activity continued overall tradecraft tendencies revealed in the Triton incident (likely the work of Gladkikh), while adding additional capabilities and tools. Based on 'multiple Triton-related incident responses carried out by FireEye Mandiant', the group continued its use of customized publicly available tools (e.g. PLINK and CryptCat). One example, linked to XENOTIME operations through several commercial malware repositories, was the malicious use of *Net Square*'s *Netexec* utility [18]. This software, which appears to no longer be supported, is a remote command execution tool functionally similar to the *Microsoft Sysinternals PsExec* utility. The publicly available binary essentially allows for remote access tool functionality in also implementing file transfer mechanisms along with process manipulation. XENOTIME appears to strongly favour the use of such tools for initial access and lateral movement activity, potentially to allow XENOTIME to 'blend in' with benign actions, or to obfuscate attribution efforts.

Following the Triton incident and the two items detailed above in this section, XENOTIME appeared to take an interesting turn from oil and gas targeting to researching electric utilities. Based on reporting from *Dragos* released in 2019, XENOTIME initiated reconnaissance and target development operations against US-based electric utilities no later than late-2018 [19, 20]. As noted in reporting and press interviews, none of the observed activity extended to active process disruption or physical destruction. But, given the nature of the Triton event, such intrusions are deeply concerning as they again represent the necessary preliminaries for such an act.

The trend of 'probing, but not exploiting' appeared to continue when comments from *Dragos* in 2022 indicated continued XENOTIME-linked operations against liquefied natural gas (LNG) operations, likely in the US [21]. Although emphasized as initial access and survey operations, the identified activity would represent continued interest by XENOTIME in US critical infrastructure operations, while also aligning with efforts to research but not (immediately) disrupt targeted networks.

Overall, as shown in the timeline in Figure 3, XENOTIME has remained active since the Triton incident in 2017. While the nature of these actions largely aligned with preparatory or preliminary operations, the group's history makes these items causes for concern. Having previously deployed a capability likely designed to remove process safety from industrial environments, even consequence-free efforts such as 'research' and 'access development' carry significant risk as initial steps towards future, far more concerning actions.

Frustratingly, the specific motivations behind the Triton event are unknown, which limits our ability to understand just what XENOTIME is tasked with achieving. As a Russian-linked incident targeting an entity in Saudi Arabia, the Triton event is especially confusing considering geopolitical matters. During the Triton incidents and subsequent investigation in 2017, Russia and Saudi Arabia engaged in significant diplomatic discussion leading to a variety of agreements and a state visit by Saudi royalty in October 2017 [22]. While such agreements frayed not long after [23], a state-sanctioned destructive attack against Saudi oil infrastructure during a period of intense diplomatic discussion seems incredibly odd – one reason why some researchers were prompted initially to link the framework to Iran [24]. Alternatively, the intrusion may have desired a pre-positioned capability to hold Saudi infrastructure at risk should such discussions fail. While making for interesting discussion, no actual evidence exists to confirm such a scenario, leaving us with little to pursue this possibility.

Given multiple public and private parties linking the event to Russia, we can be reasonably confident in associating XENOTIME to Russian entities, although based on targeting and other factors during the Triton event, links to overall Russian policy and strategic interests appear strange. Nonetheless, XENOTIME sought a physically disruptive event that could result not only in physical damage, but also direct harm to personnel onsite. Geopolitical motivations may remain confusing in this event, given a lack of tensions between Russia and Saudi Arabia compared to other areas such as Ukraine that have been the victims of Russian cyber aggression, but the implications are indisputable for potential impact scenarios.

By expanding its targeting post-2017 to the US, XENOTIME shows a continued willingness (if not yet ability) to cause havoc and potentially even direct harm. Considering these observations, a review of XENOTIME and its relationship to broader Russian-linked hacking entities is helpful to determine just who this group may be, and how TsNIIKhM may (or may not) fit in with the rest of Russian-directed offensive cyber operations.

Figure 3: Timeline of XENOTIME-linked actions.

ORGANIZATIONS AND THE CHAIN OF COMMAND

TsNIIKhM represents the 'prime mover' for Triton actions, based on analysis and reporting from multiple entities – but not the only entity involved given the lack of specificity concerning development of Triton itself. Post-2017 activity becomes murkier still, with primarily private entities – most notably *Mandiant* and *Dragos* – publicly identifying continuity from the Triton incident to follow-on actions under the XENOTIME banner, especially against US-based critical infrastructure entities. The very specific identification of Gladkikh and detailed accounting of specific actions taken by him (and unknown co-conspirators) emphasizes an operational role for TsNIIKhM and its ADC component including in non-Triton events [17], yet silence from other parties on TsNIIKhM's role in actions post-2017, despite significant warnings (and public identification of cyber operations groups) surrounding Russia's brutal invasion of Ukraine, stands out [25].

For context, TsNIIKhM is a research institution that resides (indirectly) under Russia's MOD, via the Federal Service for Technical and Export Control of Russia [26, 27]. As such, it would appear logical for activities linked to TsNIIKhM to associate with other Russian military elements such as the Main Intelligence Directorate (GRU) Main Center for Special Technologies, Field Post number 74455 – also popularly known as 'Sandworm' [28, 29]. Sandworm is linked to multiple disruptive operations, ranging from the NotPetya wiper event to the three electric disruptive incidents in Ukraine [25, 30, 31]. Given the group's track record, it would appear a natural 'fit' for an attempted destructive operation in a petrochemical facility – yet through multiple statements and actions condemning Sandworm, no entity has ever linked TsNIIKhM (or XENOTIME activity) to Sandworm.

Russia's MOD maintains an entire ecosystem of research institutes and related entities involved in various endeavours, and none of these appear directly linked to supporting active operations such as those attributed by various parties to TsNIIKhM and ADC [32]. TsNIIKhM appears to exist as just one of many organizations supporting various MOD operations and research endeavours – but one notably linked to an attempted destructive cyber attack. Moreover, TsNIIKhM engaged in precisely the operations one would associate with a military or espionage actor – initial access and capability execution, such as in Triton or the 2017-2018 US oil and gas entity incident – while remaining unlinked in any detailed analysis from where one would expect such an organization to be involved, in developing a capability such as Triton.

Furthermore, Russia's MOD does not retain absolute control over the output of military- or defence-focused labs, nor are they the only sponsor for such activity. As revealed in additional USDT sanctions, other facilities such as the Foreign Intelligence Service (SVR)-linked Federal State Autonomous Scientific Establishment Scientific Research Institute Specialized Security Computing Devices and Automation entity (SVA), and the public-private research entity ERA Technopolis also provide critical support in cyber effects capability development to multiple Russian government entities [33]. As outlined in the Treasury sanctions, these organizations provided material support to various Russian-aligned entities, including GRU and SVR elements, across several campaigns.

Russia's MOD and SVR are not alone either – in 2018, USDT sanctioned another state-sponsored research institute for operational connections with Russia's Federal Security Service (FSB) [34]. Specifically calling out cyber operations, USDT's OFAC statement singled out the Kvant Scientific Research Institute for supporting offensive actions. Based on the institute's web page, Kvant specializes in a variety of computing tasks and development work, without specifically referencing Russia's FSB or other entities [35]. Unfortunately, lack of specific details prevents us from determining the precise extent of Kvant's 'operational' support to FSB actions, but this does hint that perhaps XENOTIME and TsNIIKhM may not be as unique as initial assessments would indicate.

There thus appears to be a complex ecosystem of government-sponsored, government-aligned, and industry-linked entities intimately tied to enabling Russian-linked cyber operations. Such organizations span the 'hydra' of Russian intelligence services – FSB, GRU and SVR – although overlap or links between these entities appear limited to non-existent [36]. A key unifier in USDT OFAC statements is a focus on *supporting* roles to these agencies though, as opposed to the very direct position TsNIIKhM appears to be involved in through Gladkikh's actions under ADC. Thus, something materially different appears considering TsNIIKhM compared to other research organizations, where the organization's ADC division serves not just as a centre of expertise but also a potential reservoir of talent for operational purposes.

In comparison, SVA, ERA Technopolis, and (potentially) Kvant appear to be more traditional capability development organizations. For example, leadership of the ERA Technopolis project falls under the prestigious Kurchatov Institute, aligning it with overall Russian (military-directed) scientific pursuits [37]. This is in addition to more dual-use organizations such as the civilian-military Advanced Research Foundation (ARF), specializing in a combination of commercial and military research objectives [38]. Along with SVA and Kvant, the groups focus on developing and deploying technologies to materially improve Russian military and defence performance. Overall, Russian government (and military) investments have substantially increased across multiple 'bleeding edge' technologies, including cyber but extending to artificial intelligence, additive manufacturing, and strategic strike capabilities, which is unsurprising, except when the researchers appear to step in front of operations as Gladkikh appears to have done.

Precisely why TsNIIKhM and its ADC element would extend beyond this traditional role to active involvement thus represents a mystery. This mystery is extended to questions on what entity – MOD, GRU, or other – *tasked* TsNIIKhM to execute Triton and follow-on XENOTIME operations. While the involvement of a quasi-government research institute in significant cyber operations is hardly new (one can look at alleged examples such as the involvement of US national laboratories in Stuxnet development [39]) the involvement in direct operations is unique. A theory postulating TsNIIKhM research leading to the development of Triton itself would be easy to accept, but failing to make this attributive statement while aligning intrusion and execution activity to a TsNIIKhM employee represents an oddity.

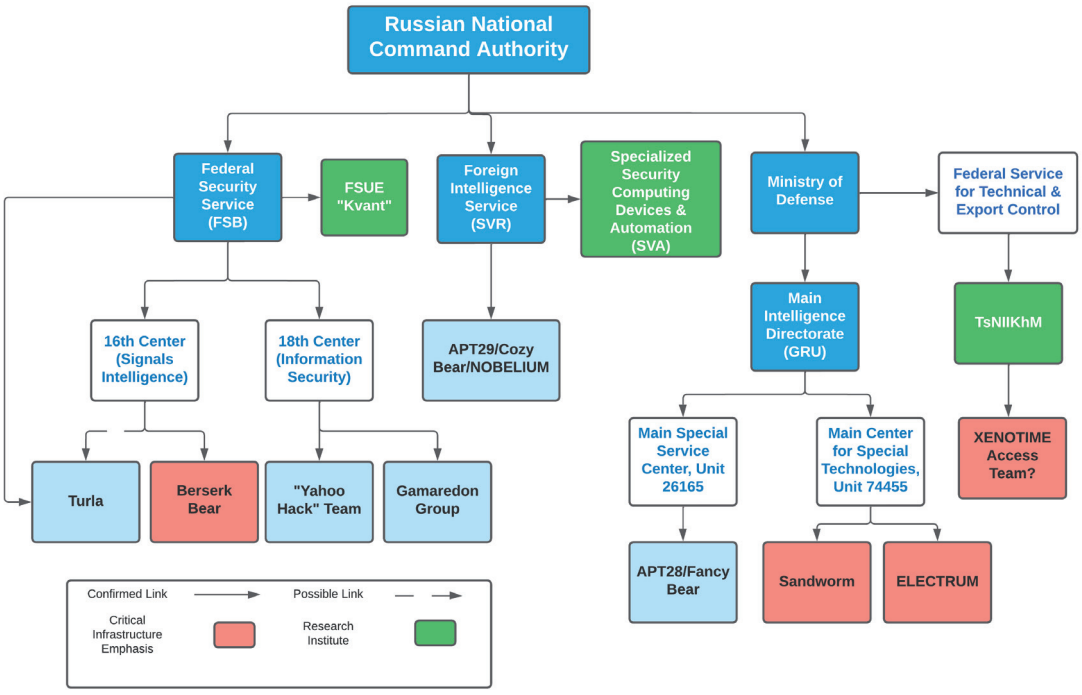

Figure 4: Overview of Russia-linked threat actors and support institutions.

OPERATORS AND DEVELOPERS

Modern, scalable cyber operations represent a complex interaction of tasks and functions. Whether described through mechanisms such as the 'Cyber Kill Chain' [40] or through references to 'digital quartermaster' scenarios [41, 42], cyber

operations represent a division of labour between experts and professionals when conducted at any type of scale or sophistication. In the case of Triton and follow-on XENOTIME events, an individual like Gladkikh may be intimately involved in initial access and follow-on lateral movement activity, but to expect the same individual also to research, develop and complete a tool such as Triton in parallel seems unreasonable, if not outright ridiculous. We thus need to differentiate between actors and deployers, and developers and researchers, where tool-specific tracking (e.g. focusing on Triton) differentiates from intrusion analysis and subsequent actions (post-2017 XENOTIME activity) [43].

XENOTIME, in this case, represents a curiosity – an entity linked to *operational* outcomes (breaching Petro Rabigh, deploying Triton, probing various other networks) but not *developmental* tasks. As such, it would appear to align closer to entities such as Sandworm or other Russian-linked cyber activity groups. But as a research institute, it would seem more aligned with preparatory and tool development actions, as noted in public reporting around entities such as SVA and Kvant. So from a researcher's perspective, what is going on?

For the purposes of XENOTIME, we as researchers must question our ability to adequately identify just what this entity *is* and *who they are*. While their *involvement* (when equating XENOTIME to TsNIIKhM) in the Petro Rabigh incident should go without question now, following multiple researcher and government disclosures, subsequent acts begin to appear murky. We must ask ourselves what distinctions exist between researchers, developers, deployers and actors. In the case of Gladkikh, it appears there was a unification of capabilities, but follow-on events present concerns as the involvement of Gladkikh (beyond the US oil and gas entity), TsNIIKhM, and the ADC division, remain unknown.

XENOTIME, essentially, may be an item adhering to *strategic interests* as opposed to a *single, specific entity*. In this sense, XENOTIME becomes a placeholder for a broader, deeper campaign linked to Russian strategic interests to develop, deploy, and enable critical infrastructure impacts. As such, TsNIIKhM is simply a *vessel* for certain actions, beholden to the command and control of some other party – whether that party is the Russian MOD, or reaches all the way to Russian national command authority, remains frustratingly unknown. Post-Triton actions tracked as XENOTIME may very well be the actions of whatever entity tasked TsNIIKhM.

From a threat research and analysis perspective, we as analysts must increasingly accept and incorporate this division of labour – even if the precise links and lines of authority remain obscured – into our analysis. XENOTIME represents one element of what is likely a much broader campaign to research, subvert, and lay the groundwork for disrupting critical infrastructure in multiple environments. Perhaps tool development resides with TsNIIKhM, or maybe this institute also, through ADC, engages in operations – but overall, the organization is merely one piece in a much larger machine using cyber actions to execute strategic goals.

Analysts must therefore diversify their understanding and expand their horizons. XENOTIME, while a useful moniker and tracking item, is an artificial construct overlaid on complex inter-agency and cross-organizational actions that most – if not all – organizations will have limited if any visibility into. From an attribution and tracking perspective, analysts should therefore accept and embrace the limitations of collection and data sourcing to understand just what is revealed to us, and what remains a mystery as we delve into development, tasking, and other relationships [44]. This is not to advise leaving such actions alone, but rather a call to understand that our insight into complex operations, with unknown sponsors and multiple executing intermediaries, represents a collection item well beyond the capability of all but the most well-resourced government intelligence agencies. XENOTIME, therefore, is a variable – a placeholder collecting a variety of actions, from Gladkikh to TsNIIKhM to the 'unnamed' entities in DOJ indictments, and not a unitary, specific, and well-defined entity in the world.

CONCLUSIONS

The 2017 Triton incident represents a seminal moment in cyber operations, as this is the first (known) incident where a threat actor sought to undermine fundamental process safety in a cyber-physical event. As such, Triton remains a critical touchpoint in threat analysis and research, even if the attack likely failed in its objectives given the recorded results. However, the entity (or entities) responsible, tracked under the moniker of XENOTIME, remained active beyond the incident at Petro Rabigh. XENOTIME thus emerged as a persistent, concerning threat to critical infrastructure spanning continents given the entity's link to physically disruptive, potentially life-threatening outcomes.

Yet in grasping XENOTIME and understanding what this entity really 'is', we face a question – while direct relationship with TsNIIKhM (and its ADC division) is convenient and helpful, further analysis of events reveals a far murkier picture. While certainly possible, an organization such as TsNIIKhM engaging in offensive, potentially destructive operations on its own accord is not merely curious, but ridiculous within the greater ecosystem of Russia-controlled cyber operations. Instead, TsNIIKhM represents a player in a far wider game with multiple participants engaged in potentially destructive operations for ends unknown.

For threat researchers and analysts, the above may appear as so much trivial detail, but a more robust understanding of how complex cyber operations are conducted indicates 'messy' situations like Triton and XENOTIME are likely to be the norm for future events. Looking at incidents, particularly those associated with state-directed operations, as a combination of efforts across multiple entities reveals the truth of such events, as composites stretching from research institutes such as TsNIIKhM to known elements such as GRU or SVR. While Triton and XENOTIME appear to subvert some of the

expectations around these relationships, with ADC and Gladkikh engaged in very active operations, the underlying trend of a division of labour remains.

XENOTIME thus represents less a monolithic actor than a composite of multiple stakeholders acting on the behalf of a national command authority to subvert critical infrastructure functionality. Triton, as worrying as the event may be, could be considered a preview of future operations as the entities subsumed under the XENOTIME label expanded their efforts to multiple critical infrastructure entities. By understanding these relationships (and the dependencies they engender), we as threat analysts and defenders can better appreciate the level of effort involved in such operations, and the need to differentiate between the entities on the keyboard and who their ultimate masters may be.

REFERENCES

[1] 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/.

[2] Gutmanis, J. Triton – A Report from the Trenches. YouTube. 11 March 2019. https://www.youtube.com/watch?v=XwSJ8hloGvY.

[3] Johnson, B.; Caban, D.; Krotofil, M.; Scali, D.; Brubaker, N.; Glyer, 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.

[4] Dragos. TRISIS Malware: Analysis of Safety System Targeted Malware. 13 December 2017. https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf.

[5] US Cybersecurity and Infrastructure Security Agency. MAR-17-352-01 HatMan – Safety System Targeted Malware (Update B). 27 February 2019. https://www.cisa.gov/uscert/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf.

[6] 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.

[7] US Department of the Treasury. Treasury Sanctions Russian Government Research Institution Connecfted to the Triton Malware. 23 October 2020. https://home.treasury.gov/news/press-releases/sm1162.

[8] Nakashima, E., Gregg, A. They're on the lookout for malware that can kill. Washington Post. 27 April 2018. https://www.washingtonpost.com/world/national-security/theyre-on-the-lookout-for-malware-that-can-kill/2018/04/27/33190738-32c1-11e8-8abc-22a366b72f2d_story.html.

[9] Dragos. XENOTIME. https://www.dragos.com/threat/xenotime/.

[10] 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.

[11] 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.

[12] Wightman, R.; Wylie, J. Analyzing TRISIS. Vimeo. 2018. https://vimeo.com/275906105.

[13] Wetzels, J. Analyzing the TRITON Industrial Malware. Midnight Blue Labs. 16 January 2018. https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware.

[14] 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.

[15] TsNIIKhM. Scientific Directions. 31 March 2022. https://web.archive.org/web/20220331220927/https://cniihm.ru/.

[16] TsNIIKhM. Applied Development Center. 16 February 2018. https://web.archive.org/web/20180216050244/http:/cniihm.ru:80/about/napravlenie/tspr/.

[17] 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.

[18] NetSquare. netexec - Remote Command Execution. 04 April 2019. https://web.archive.org/web/20190409005254/http://www.net-square.com/nstools.html.

[19] Dragos. Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas. 14 June 2019. https://www.dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/.

[20] Lyngaas, S. The group behind Trisis has expanded its targeting to the U.S. electric sector. CyberScoop. 14 June 2019. https://www.cyberscoop.com/trisis-xenotime-us-electric-sector/.

[21] Lyngaas, S. US officials prepare for potential Russian cyberattacks as Ukraine standoff continues. CNN. 02 Feb 2022. https://www.cnn.com/2022/02/02/politics/fbi-ukraine-cyber-russia/index.html.

[22] Soldatkin, V.; Golubkova, K. Russia, Saudi Arabia cement new friendship with king's visit. Reuters. 05 October 2017. https://www.reuters.com/article/us-russia-saudi-terror/russia-saudi-arabia-cement-new-friendship-with-kings-visit-idUSKBN1CA1QU.

[23] Higgins, A.; Kramer, A. E. Behind the Russia-Saudi Breakup, Calculations and Miscalculations. New York Times. 10 March 2020. https://www.nytimes.com/2020/03/10/world/europe/russia-saudi-oil.html.

[24] Paganini, P. Titon Malware was Developed by Iran and Used to Target Saudi Arabia. Security Affairs. 16 December 2017. https://securityaffairs.co/wordpress/66784/malware/triton-malware-iran.html.

[25] US Cyber Security and Infrastructure Security Agency. Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. 09 May 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

[26] TsNIIKhM. HISTORY OF THE FEDERAL STATE UNITARY ENTERPRISE "TSNIIKHM". https://cniihm.ru/%d0%b8%d1%81%d1%82%d0%be%d1%80%d0%b8%d1%8f/.

[27] FSTEC. FSTEC Russia. https://fstec.ru/en/358-structure.

[28] US National Security Agency. Sandworm Actors Exploiting Vulnerability in EXIM Mail Transfer Agent. 28 May 2020. https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA-Sandworm-Actors-Exploiting-Vulnerability-in-Exim-Transfer-Agent-20200528.pdf.

[29] US Department of Justice. Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace. 19 October 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[30] UK National Cyber Security Centre. Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed. 03 October 2018. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

[31] ESET Research. Industroyer2: Industroyer Reloaded. 12 April 2022. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

[32] Ministry of Defence of the Russian Federation. Scientific Research Organizations. 04 April 2022. https://web.archive.org/web/20220404071513/https://eng.mil.ru/en/science/sro.htm.

[33] US Department of the Treasury. Treasury Sanctions Russia with Sweeping New Sanctions Authority. 15 April 2021. https://home.treasury.gov/news/press-releases/jy0127.

[34] US Department of the Treasury. Treasury Sanctions Russian Federal Security Service Enablers. 11 June 2018. https://home.treasury.gov/news/press-releases/sm0410.

[35] Federal State Unitary Enterprise Research Institute "Kvant". Kvant – Activities. https://www.rdi-kvant.ru/?page_id=47.

[36] Galeotti, M. Putin's Hyrda: Inside Russia's Intelligence Services. European Council of Foreign Relations. 11 May 2016. https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf.

[37] Nikolsky, A. Lofty Goals. Force India. https://forceindia.net/cover-story/lofty-goals/.

[38] Bendett, S.; Boulègue, M.; Connolly, R.; Konaev, M.; Podvig, P.; Zysk, K. Advanced Military Technology in Russia: Capabilities and Implications. Chatham House. September 2021. https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-23-advanced-military-technology-in-russia-bendett-et-al.pdf.

[39] Zetter, K. Did a U.S. Government Lab Help Israel Develop Stuxnet. Wired. 17 January 2011. https://www.wired.com/2011/01/inl-and-stuxnet/.

[40] Hutchins, E. M.; Cloppert, M. J.; Amin, R. M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

[41] Grunzweig, J.; Falcone, R.; Lee, B. Digital Quartermaster Scenario Demonstrated in Attacks Against the Mongolian Government. Palo Alto Networks. 14 March 2016. https://unit42.paloaltonetworks.com/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/.

[42] Mandiant. Supply Chain Analysis: From Quartermaster to SunshopFireEye. September 2021. https://www.mandiant.com/sites/default/files/2021-09/rpt-malware-supply-chain.pdf.

[43] Slowik, J. Threat Intelligence and the Limits of Malware Analysis. Dragos. January 2020. https://www.dragos.com/wp-content/uploads/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf.

[44] Slowik, J. Conceptualizing a Continuum of Cyber Threat Attribution. Domain Tools. https://www.domaintools.com/content/conceptualizing-a-continuum-of-cyber-threat-attribution.pdf.