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

By Mandiant

Published: 2018-10-23 · Archived: 2026-04-05 12:42:38 UTC

Written by: FireEye Intelligence

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 surrounding the TRITON intrusion to a Russian government-owned research institute.

TRITON Intrusion Demonstrates Russian Links; Likely Backed by Russian Research Institute

FireEye Intelligence assesses with high confidence that intrusion activity that led to deployment of TRITON was supported by the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM; a.k.a. ЦНИИХМ), a Russian government-owned technical research institution located in Moscow. The following factors supporting this assessment are further detailed in this post. We present as much public information as possible to support this assessment, but withheld sensitive information that further contributes to our high confidence assessment.

1. FireEye uncovered malware development activity that is very likely supporting TEMP.Veles activity. This includes testing multiple versions of malicious software, some of which were used by TEMP.Veles during the TRITON intrusion.
2. Investigation of this testing activity reveals multiple independent ties to Russia, CNIIHM, and a specific person in Moscow. This person's online activity shows significant links to CNIIHM.
3. An IP address registered to CNIIHM has been employed by TEMP.Veles for multiple purposes, including monitoring open-source coverage of TRITON, network reconnaissance, and malicious activity in support of the TRITON intrusion.
4. Behavior patterns observed in TEMP.Veles activity are consistent with the Moscow time zone, where CNIIHM is located.
5. We judge that CNIIHM likely possesses the necessary institutional knowledge and personnel to assist in the orchestration and development of TRITON and TEMP.Veles operations.

While we cannot rule out the possibility that one or more CNIIHM employees could have conducted TEMP.Veles activity without their employer's approval, the details shared in this post demonstrate that this explanation is less plausible than TEMP.Veles operating with the support of the institute.

Detail

Malware Testing Activity Suggests Links between TEMP.Veles and CNIIHM

During our investigation of TEMP.Veles activity, we found multiple unique tools that the group deployed in the target environment. Some of these same tools, identified by hash, were evaluated in a malware testing environment by a single user.

Malware Testing Environment Tied to TEMP.Veles

We identified a malware testing environment that we assess with high confidence was used to refine some TEMP.Veles tools.

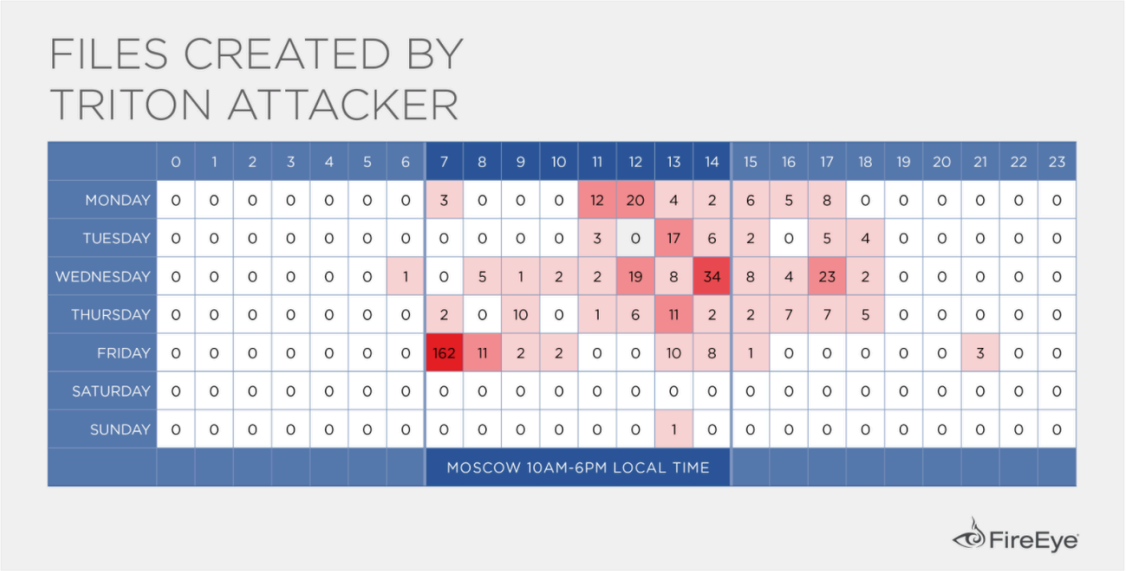
- At times, the use of this malware testing environment correlates to in-network activities of TEMP.Veles, demonstrating direct operational support for intrusion activity.
    - Four files tested in 2014 are based on the open-source project, cryptcat. Analysis of these cryptcat binaries indicates that the actor continually modified them to decrease AV detection rates. One of these files was deployed in a TEMP.Veles target's network. The compiled version with the least detections was later re-tested in 2017 and deployed less than a week later during TEMP.Veles activities in the target environment.
    - TEMP.Veles' lateral movement activities used a publicly-available PowerShell-based tool, WMImplant. On multiple dates in 2017, TEMP.Veles struggled to execute this utility on multiple victim systems, potentially due to AV detection. Soon after, the customized utility was again evaluated in the malware testing environment. The following day, TEMP.Veles again tried the utility on a compromised system.
- The user has been active in the malware testing environment since at least 2013, testing customized versions of multiple open-source frameworks, including Metasploit, Cobalt Strike, PowerSploit, and other projects. The user's development patterns appear to pay particular attention to AV evasion and alternative code execution techniques.
- Custom payloads utilized by TEMP.Veles in investigations conducted by Mandiant are typically weaponized versions of legitimate open-source software, retrofitted with code used for command and control.

Testing, Malware Artifacts, and Malicious Activity Suggests Tie to CNIIHM

Multiple factors suggest that this activity is Russian in origin and associated with CNIIHM.

- A PDB path contained in a tested file contained a string that appears to be a unique handle or user name. This moniker is linked to a Russia-based person active in Russian information security communities since at least 2011.
    - The handle has been credited with vulnerability research contributions to the Russian version of Hacker Magazine (хакер).
    - According to a now-defunct social media profile, the same individual was a professor at CNIIHM, which is located near Nagatinskaya Street in the Nagatino-Sadovniki district of Moscow.

    - Another profile using the handle on a Russian social network currently shows multiple photos of the user in proximity to Moscow for the entire history of the profile.
- Suspected TEMP.Veles incidents include malicious activity originating from 87.245.143.140, which is registered to CNIIHM.
    - This IP address has been used to monitor open-source coverage of TRITON, heightening the probability of an interest by unknown subjects, originating from this network, in TEMP.Veles-related activities.
    - It also has engaged in network reconnaissance against targets of interest to TEMP.Veles.
    - The IP address has been tied to additional malicious activity in support of the TRITON intrusion.
- Multiple files have Cyrillic names and artifacts.



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MONDAY	0	0	0	0	0	0	0	3	0	0	0	12	20	4	2	6	5	8	0	0	0	0	0	0
TUESDAY	0	0	0	0	0	0	0	0	0	0	0	3	0	17	6	2	0	5	4	0	0	0	0	0
WEDNESDAY	0	0	0	0	0	0	1	0	5	1	2	2	19	8	34	8	4	23	2	0	0	0	0	0
THURSDAY	0	0	0	0	0	0	0	2	0	10	0	1	6	11	2	2	7	7	5	0	0	0	0	0
FRIDAY	0	0	0	0	0	0	0	162	11	2	2	0	0	10	8	1	0	0	0	0	0	3	0	0
SATURDAY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SUNDAY	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0

Figure 1: Heatmap of TRITON attacker operating hours, represented in UTC time

Behavior Patterns Consistent with Moscow Time Zone

Adversary behavioral artifacts further suggest the TEMP.Veles operators are based in Moscow, lending some further support to the scenario that CNIIHM, a Russian research organization in Moscow, has been involved in TEMP.Veles activity.

- We identified file creation times for numerous files that TEMP.Veles created during lateral movement on a target's network. These file creation times conform to a work schedule typical of an actor operating within a UTC+3 time zone (Figure 1) supporting a proximity to Moscow.

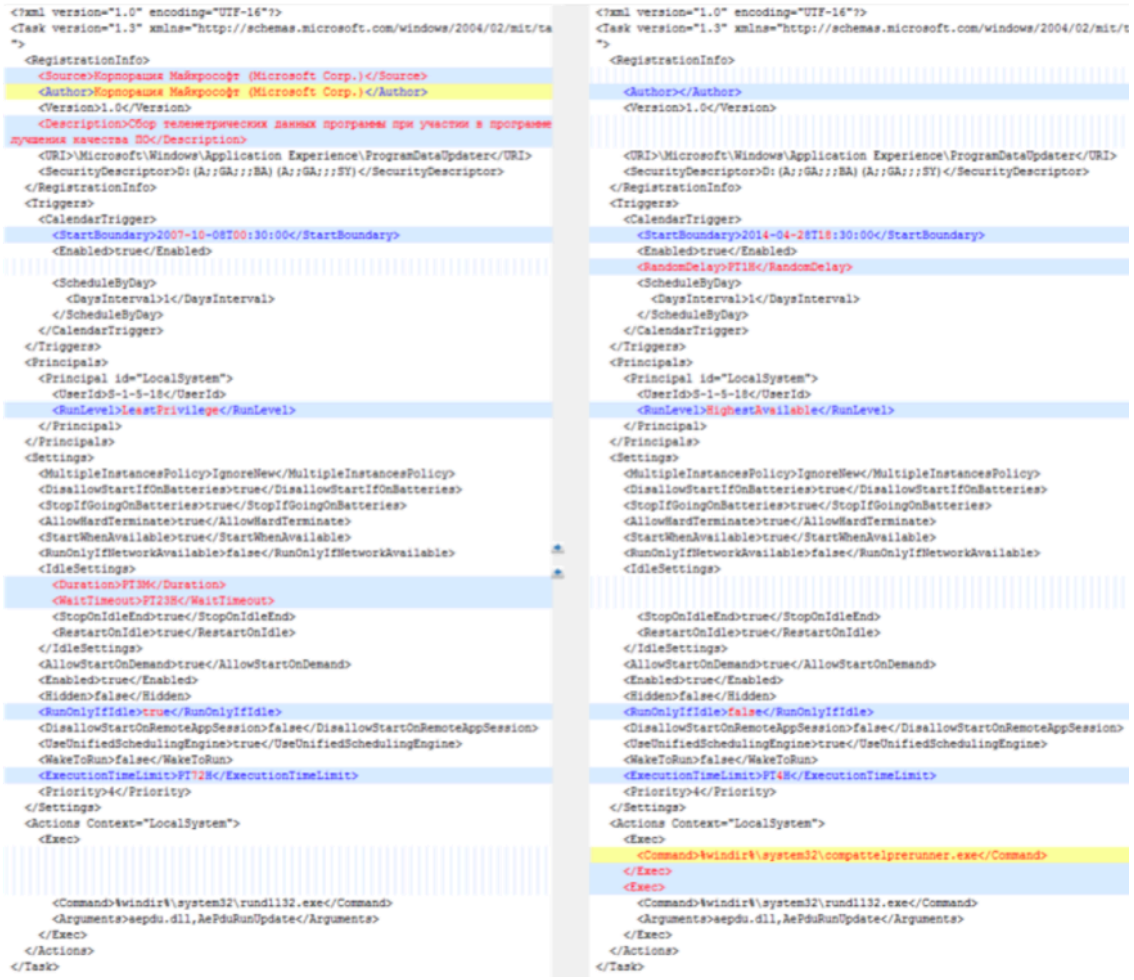


Figure 2: Modified service config

- Additional language artifacts recovered from TEMP.Veles toolsets are also consistent with such a regional nexus.
    - A ZIP archive recovered during our investigations, schtasks.zip, contained an installer and uninstaller of CATRUNNER that includes two versions of an XML scheduled task definitions for a masquerading service ‘ProgramDataUpdater.’
    - The malicious installation version has a task name and description in English, and the clean uninstall version has a task name and description in Cyrillic. The timeline of modification dates within the ZIP also suggest the actor changed the Russian version to English in sequential order, heightening the possibility of a deliberate effort to mask its origins (Figure 2).

Figure 3: Central Research Institute of Chemistry and Mechanics (CNIIHM) (Google Maps)

CNIIHM Likely Possesses Necessary Institutional Knowledge and Personnel to Create TRITON and Support TEMP.Veles Operations

While we know that TEMP.Veles deployed the TRITON attack framework, we do not have specific evidence to prove that CNIIHM did (or did not) develop the tool. We infer that CNIIHM likely maintains the institutional expertise needed to develop and prototype TRITON based on the institute's self-described mission and other public information.

- CNIIHM has at least two research divisions that are experienced in critical infrastructure, enterprise safety, and the development of weapons/military equipment:
    - The Center for Applied Research creates means and methods for protecting critical infrastructure from destructive information and technological impacts.
    - The Center for Experimental Mechanical Engineering develops weapons as well as military and special equipment. It also researches methods for enabling enterprise safety in emergency situations.
- CNIIHM officially collaborates with other national technology and development organizations, including:
    - The Moscow Institute of Physics and Technology (PsyTech), which specializes in applied physics, computing science, chemistry, and biology.
    - The Association of State Scientific Centers "Nauka," which coordinates 43 Scientific Centers of the Russian Federation (SSC RF). Some of its main areas of interest include nuclear physics, computer science and instrumentation, robotics and engineering, and electrical engineering, among others.
    - The Federal Service for Technical and Export Control (FTEC) which is responsible for export control, intellectual property, and protecting confidential information.
    - The Russian Academy of Missile and Artillery Sciences (PAPAH) which specializes in research and development for strengthening Russia's defense industrial complex.

- Information from a Russian recruitment website, linked to CNIIHM's official domain, indicates that CNIIHM is also dedicated to the development of intelligent systems for computer-aided design and control, and the creation of new information technologies (Figure 4).

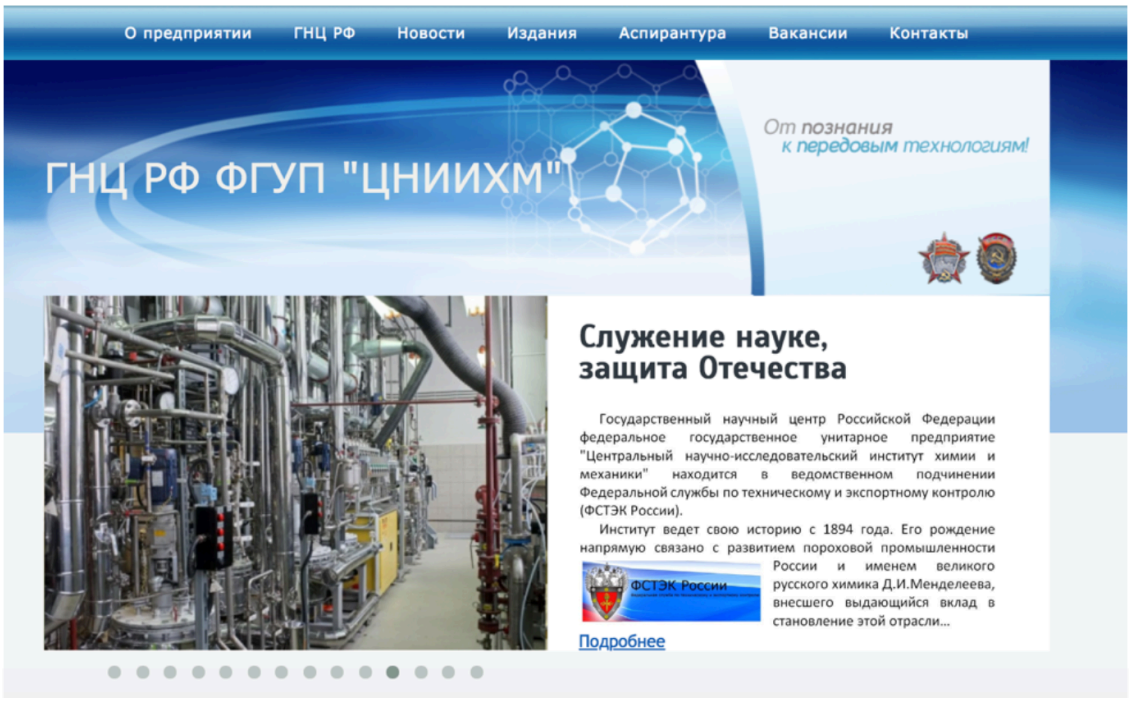


Figure 4: CNIIHM website homepage

Primary Alternative Explanation Unlikely

Some possibility remains that one or more CNIIHM employees could have conducted the activity linking TEMP.Veles to CNIIHM without their employer's approval. However, this scenario is highly unlikely.

- In this scenario, one or more persons – likely including at least one CNIIHM employee, based on the moniker discussed above – would have had to conduct extensive, high-risk malware development and intrusion activity from CNIIHM's address space without CNIIHM's knowledge and approval over multiple years.
- CNIIHM's characteristics are consistent with what we might expect of an organization responsible for TEMP.Veles activity. TRITON is a highly specialized framework whose development would be within the capability of a low percentage of intrusion operators.

Posted in

- Threat Intelligence
- Security & Identity
