Dataminr

Determining Volt Typhoon Next Steps & Defensive Responses

Joseph Slowik

Abstract

Volt Typhoon (VT) emerged as a leading threat to critical national infrastructure (CNI) entities over the past five years, with public sourcing identifying breaches at multiple organizations in strategic geographies or sectors. Yet for all the concern relating to VT operations, no follow-on actions or impact scenarios, whether in IT or OT environments, have been linked to this entity. As a result, CNI owners and defenders face an extremely uncertain landscape for precisely how to detect, defend, and mitigate against a prospective VT intrusion leading to an impact scenario.

In this discussion, we will examine a combination of identified VT tradecraft and how this aligns with known impact scenarios in CNI environments to identify plausible follow-on actions from VT breaches. Leveraging historical analysis and understanding of adversary capabilities, we can identify likely VT actions and objectives in CNI intrusions. Through this assessment, we will identify high-probability VT next steps to guide and focus defensive resource allocation, as well as resilience strategies, closing significant defender awareness and understanding gaps. In documenting these actions, we will also identify weaknesses in current behavioral mapping frameworks, how entities like VT pose unique problems for threat intelligence analysis given their partial manifestation in terms of kill chain analysis, and how existing analytical frameworks must evolve in the face of threats such as VT.

Introduction

Volt Typhoon (VT) is a threat actor first publicly disclosed in 2023 by multiple parties, with some assessments indicating the group may have been active as early as 2019.

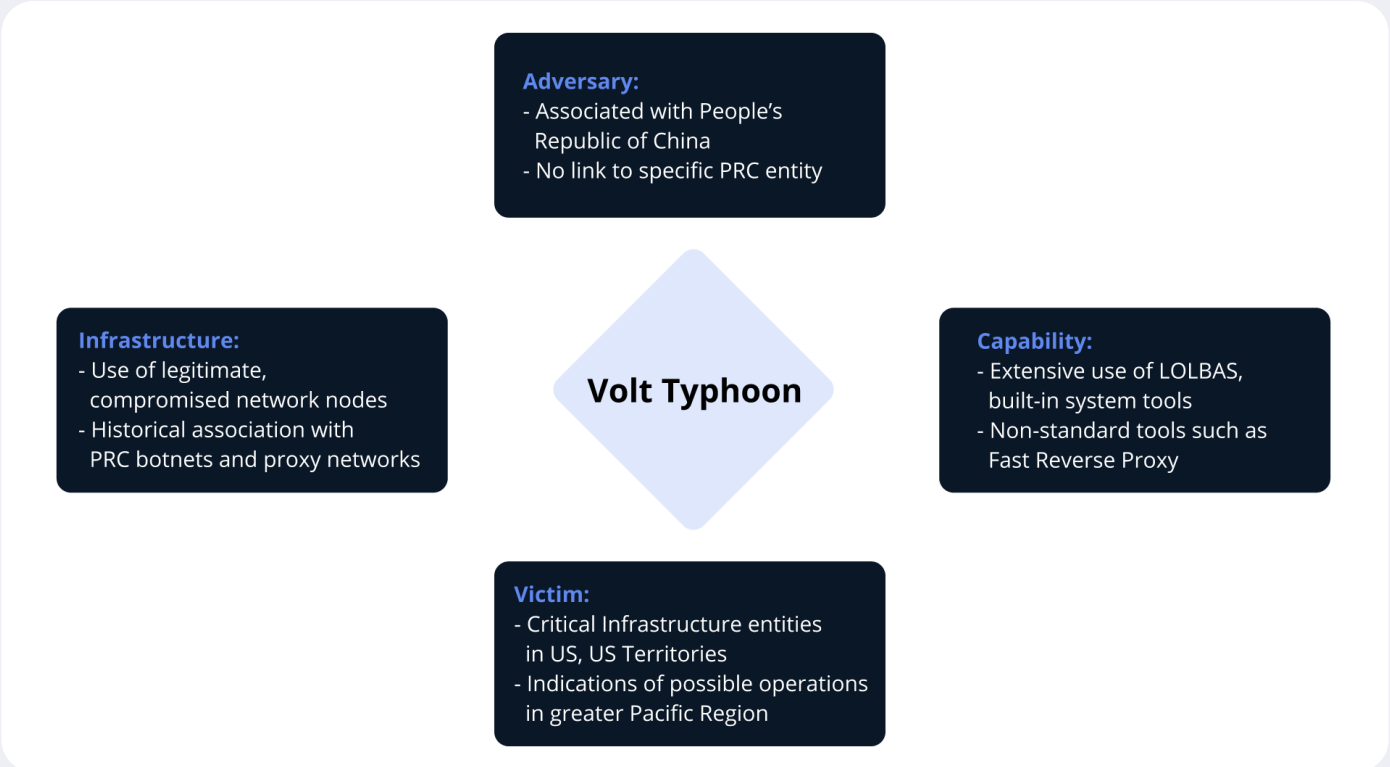


Figure 1: Diamond Model Analysis of Volt Typhoon

Linked to unspecified entities operating out of the People's Republic of China (PRC), VT actions have predominantly targeted various critical infrastructure entities in the United States (US). VT activity is well-categorized from an IT intrusion and lateral movement perspective, as shown in Figure 1. However, although targeting critical national infrastructure (CNI) entities that typically feature industrial and operational technology (OT) environments, VT's actions and intentions are less understood from a cyber-physical attack scenario perspective.

Notably, VT has operated against multiple entities with OT environments, such as reported actions against a small utility in the US,[1] yet there is no known, disruptive or similar event linked to VT intrusions. One likely reason for this may be the assessed nature of VT's mission: to develop and prepare for *future* disruptive events, as opposed to engaging in *immediate* attacks.

While specific VT-linked incidents or OT events are lacking, analysts can still forecast likely VT actions to achieve or enable subsequent cyber-physical impact scenarios. Through a combination of VT-specific behavioral analysis and evaluation of historical OT-targeting events, analysts and defenders can develop a grounded profile of future VT activity. First, all available evidence on VT operations indicates the group prefers a combination of Living off the Land Binary and Script (LOLBAS) use to generally evade detection and "blend in" with normal system operations, with some additional use of less-common tools such as Fast Reverse Proxy (FRP) to enable specific operational elements.[2] Based on these IT-centric trends, we can infer that similar methodology would be used in OT network intrusions: LOLBAS use, largely fueled through harvested, legitimate credentials supplemented with occasional non-standard tools for specific outcomes.

From this we can begin to formulate a plan of action to identify or counter VT actions to share with defenders for threat emulation and detection purposes. While we should be cautious of over-projecting from known VT IT tradecraft to OT operations, the combination of evidence from known VT actions and historical OT intrusions leveraging similar methodology (e.g., operations leading up to the 2016 Ukraine power incident[3]) show that credential harvesting followed by native system application use remains a popular and potent intrusion mechanism.

In addition to these forecasted behaviors, aligning with OT intrusion and subsequent lateral movement, there is also the question of actual OT effects and cyber-physical payload use to achieve a potential disruptive (or destructive) impact. For OT-based cyber effects, there is no data associated with VT operations to use for forecasting purposes. However, we can assess based on reported VT tradecraft that VT is aware of and closely tracks publicly reported items in security operations. Therefore, previously documented OT intrusions can provide a baseline against which to assess future VT actions within OT spaces, identifying both available attack vectors as well as learning from noted mistakes made by historical adversaries.

Through the above plan of action, a VT-focused assessment can be created for likely, future OT operations. Using this evaluation, OT asset owners and defenders can begin developing prioritized plans for improving visibility and monitoring, along with detection deployment and response to counter potential VT cyber-physical actions in networks of interest.

Volt Typhoon Lateral Movement & Process Execution

VT actions observed in IT environments, as documented by the US Cybersecurity and Infrastructure Security Agency (CISA), Microsoft, and Secureworks aligns with known adversary tradecraft in OT access and lateral movement operations.[4][5][6] Available assessments of VT activity indicate the group relies on credential harvesting followed by LOLBAS activity to maintain operational security while blending in with the perceived "noise" of normal network activity. Such actions have proven very effective in defense evasion in IT environments. For OT environments, that typically feature significantly less monitoring and visibility, such actions may be effectively invisible to defenders.

The use of LOLBAS and related mechanisms for OT intrusions is not new, but represents a trend going back to the mid-2010s.[7] As revealed in public analysis of the 2016 Ukraine power incident, the Sandworm threat actor relied almost exclusively on abuse of captured credentials and native system utilities to enable the OT phase of operations eventually leading to the deployment of Industroyer malware.[8] Such behaviors are reflected in subsequent OT-targeting intrusions, such as the Berserk Bear-related "Palmetto Fusion" campaign and related items linked to this entity through the early 2020s.[9][10] With the lack of endpoint detection and monitoring on most hosts within OT environments, actions such as the Sandworm and Berserk Bear activities may be invisible to defenders. Furthermore, even when some degree of event log or similar monitoring is,

available, the level of detail needed to differentiate between legitimate, benign use of system tools and suspicious or malicious activity is lacking (e.g., command switches, flags, and specific syntax). With VT already employing similar methodology in IT network intrusions to great effect, available evidence and historical perspectives strongly suggest the group will continue to operate in similar fashion for OT intrusions.

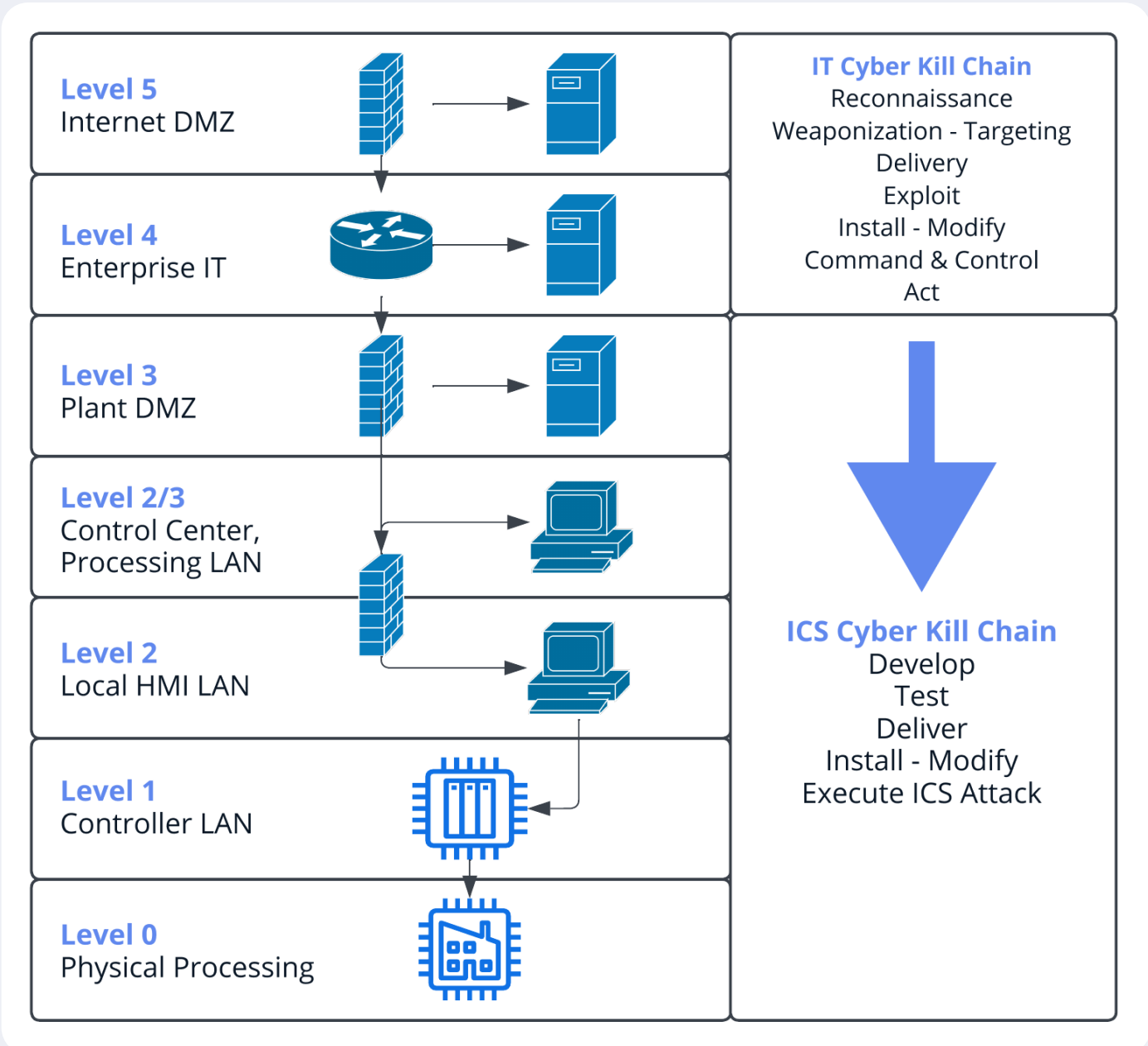
Another element to consider, going beyond host-focused actions, is VT's use of complex proxy networks to enable command and control (C2) in victim environments. VT operations are linked to extensive use of compromised, legitimate devices to proxy C2 traffic between VT itself and victims, similar to other PRC-nexus threat actors.[11] VT has used third-party botnets, such as the KV Botnet, since 2022 and potentially through various disruptive efforts on the part of US entities beginning in 2024.[12] [13] [14] Use of such proxy networks extend difficulties for defenders in identifying and countering VT-based activity as network nodes linked to intrusions are essentially ephemeral and can be rapidly changed to evade blocks and similar mechanisms. Such C2 activity would continue through the OT-focused phase of VT operations and provide for a stealthy, difficult to detect mechanism to enable remote operations in victim environments.

Existing understanding of VT actions against IT networks thus remains informative and relevant for likely initial phases of VT actions in OT environments. It is, however, possible that in response to significant public exposure VT could change its behaviors to evade defenders and counter expectations. Yet, as demonstrated by historical events going back nearly a decade, VT's core intrusion behaviors and tradecraft remain extremely problematic for defenders and system owners to counter, thus providing little incentive for VT to change even if some of these mechanisms have been identified. As a result, we should anticipate VT to continue leveraging credential theft and LOLBAS mechanisms should intrusions progress into OT environments as viewed through the ICS Cyber Kill Chain.

Unfortunately, simply saying "VT uses LOLBAS mechanisms" is insufficient to build a complete profile of the adversary, and most public reporting has largely failed to provide sufficient information on specific command and tool use that would enable the creation of robust identifiers or detectors. For example, intrusions identified either simply note LOLBAS use in general, or highlight the use of various system commands without providing specific syntax, sequencing, or other factors that may enable identification of VT-specific behaviors.[16] [17] Such information may exist, but a combination of victim privacy, intelligence equities, and poor sharing mechanism may render them unavailable in open (or at least unclassified) forums. These information gaps present significant difficulties for distinguishing between VT actions and other malicious actors, or even legitimate system administration activity.

Despite these difficulties, enough data remains available that we can assess VT objectives and outcomes from identified commands, even if insufficient data exists to create VT-specific detections and analytics to identify such activities as they take place. Based on available information, a combination of aggressive and continuous

Figure 2: ICS Cyber Kill Chain[15]



credential harvesting with repeated network survey and reconnaissance activity should be minimally expected during initial OT network intrusions. Credential capture via tools such as the near-ubiquitous Mimikatz, dumping the critical NTDS.dit file from victim domain controllers, and other mechanisms for dumping passwords from repositories will likely play a critical role in this activity, with operator reuse of passwords from already-breached IT environments providing VT with additional opportunities. Combined with legitimate administration utilities and commands, VT can place itself in a position to propagate within OT environments, while also setting itself up for the delivery of OT-specific effects packages.

Volt Typhoon Impact Scenarios

While some public reporting on VT activity indicates access to OT environments along with exfiltration of OT-related information from IT environments,[18] [19] there is no substantial, detailed public reporting on OT-focused intrusion methodologies, lateral movement, or capability deployment for VT at this time. However, based on analysis of VT's IT operations and likely awareness and understanding of past OT-focused intrusions, analysts can hypothesize likely courses of action for VT to impact CNI and related infrastructure.

VT's actions will ultimately be dependent on tasking from PRC leadership, given public attribution of the group and targeting of CNI resources. While statements from government entities and similar stress a desire to target CNI, such as logistics and energy sectors,[20] precisely how and for what specific purpose remains uncertain. While this remains concerning, and the assessments appear to be consensus opinions of informed entities speaking to the VT threat, there are many specific actions and possibilities under this very general characterization.

The actions required to simply disrupt ongoing operations in CNI will differ from those aimed at inflicting prolonged physical damage. While disruption and destruction share many commonalities in earlier phase operations prior to effect deployment, they diverge significantly in terms of capabilities required for mission accomplishment and how these need to be delivered and executed. Public reporting on VT is thus indeterminate as to what the threat actor's ultimate purposes may be, even in the event of a US-PRC conflict associated with a Taiwan Strait scenario, the most often-cited situation in which VT points of access are assessed to "go active."[21]

Analysts can, however, map out OT intrusions and attack possibilities based on a combination of historical analysis of past intrusions and current capabilities available to OT-targeting adversaries. Based on this historical review, several options for VT activity emerge that, with improved understanding and intelligence, can be narrowed to determine actual areas of focus and emphasis. By understanding and applying this combination of historical awareness and current tradecraft analysis, asset owners and defenders can begin outlining potential VT-driven OT attack scenarios.

Availability: Operational Disruption

The most direct (and simple) action VT could take against an OT environment would be immediate operational disruption. This can be achieved through IT-centric capabilities in OT environments, such as the deployment of wiping malware (including repurposed ransomware) against IT-like assets in OT networks. Alternatively, VT could simply interact with available OT controls once gaining access to systems of interest to "turn off" functionality or otherwise inhibit normal operations. The latter seems especially relevant for VT operations given the adversary's extensive use of credential harvesting and re-use in victim environments, allowing VT to access OT controls legitimately for malicious purposes. In this scenario,[22] VT can simply authenticate to a system to manipulate or disable a process.

Similar to the 2015 Ukraine incident that also featured manual manipulation of CNI assets to induce the initial impact scenario, such operations can be immediately effective but are also difficult to coordinate and scale for a widespread attack scenario.

Alternatively, a type of "blunt force" attack could be executed higher up the technical stack in a more scalable fashion. IT-based wiping malware is widespread in availability and has already featured in multiple CNI incidents, from the Shamoon (IT-focused) events in Saudi Arabia,[23] [24] to the use of KillDisk malware in both the 2015 and 2016 Ukraine events,[25] [26] to the use of CaddyWiper malware in the 2022 Industroyer2 attempt.[27] Wiping malware is relatively simplistic in capability, easy to develop, and impactful even if absent targeting of OT-specific assets. In addition to the immediate disruptive effect of inducing loss of control and loss of view conditions with the loss of IT-like OT assets, there is also the prolonged impact of impaired system operations and restoration as impacted assets likely need to be completely rebuilt and reconfigured.

While these scenarios are certainly impactful, their technical sophistication and complexity is relatively low as the capabilities necessary to execute such attacks already exist, or are easily acquired. This "lack of sophistication" is hardly a drawback, but highlights the relative ease in this attack scenario. There are, however, limiting factors to this type of direct disruption. Wiping actions face limitations in access and execution: having access to the right assets to deliver and execute a capability at the right time to ensure operational disruption aligned with adversary desires. Furthermore, such actions would need to be reasonably widespread across CNI entities and triggered roughly simultaneously for maximum effect, additional barriers in execution and control that induce friction into potential VT actions.

In these scenarios, VT would need to satisfy the following criteria for mission success:

1. Establish access to desired victim OT environments through pre-existing IT compromise.
2. Push a wiping capability into the OT environment from available C2 nodes.
3. Ensure near-concurrent execution across assets and potentially different victims to enable significant, system-wide disruption.

The first item is likely already met in existing VT actions, although definitive proof is not publicly available aside from a few media stories. VT's continuing harvesting of victim credentials and subversion of victim networks mean this access is likely a low barrier to overcome. However, access does not necessarily mean access of a degree necessary to ensure widespread distribution of an effects package across CNI victims to attain operationally significant impacts. VT would almost certainly need to engage in follow-on lateral movement and ensure persistence against a variety of OT environment assets to enable a significant impact scenario. Such an action would likely be achieved only through "hands on keyboard" actions leveraging existing credentials or other access mechanisms to build a presence within the OT environment, and as such would be time consuming and labor intensive to achieve.

Integrity: Safety & Protection Subversion

Direct damage to CNI assets, especially OT elements, is significantly more difficult and challenging than mere disruption of inducing "logical" impacts such as loss of view or even loss of control conditions. In these circumstances, adversaries need not only satisfy the same intrusion and execution stages of access, persistence, and delivery as disruptive scenarios, but must proceed further to achieve the following:

1. Identify and subvert critical logical assets with control over physical systems (e.g., PLCs, RTUs, or safety and protection systems).
2. Develop and deploy capabilities that can interact with these systems in a way that understands the fundamental process involved to manipulate that process's fundamental physics to create a damage or destruction scenario.
3. Overcome the logical and engineering process protection and safety controls to allow that capability to propagate beyond protection and safety layers, as illustrated in Figure 3, to achieve an impact.

The above items represent a far more challenging prospect than mere disruption, and as a result we have witnessed far fewer such (attempted) events than direct OT disruption. At present, only three such events exist in open source resources: the Stuxnet event, the 2016 Ukraine incident when viewed as a protection attack, and the 2017 Triton intrusion.[33] Of these, only the Stuxnet event can be viewed as "successful," highlighting that these types of multi-tiered intrusions involving engineering controls and physical safeguards represent another species of attack scenario entirely.

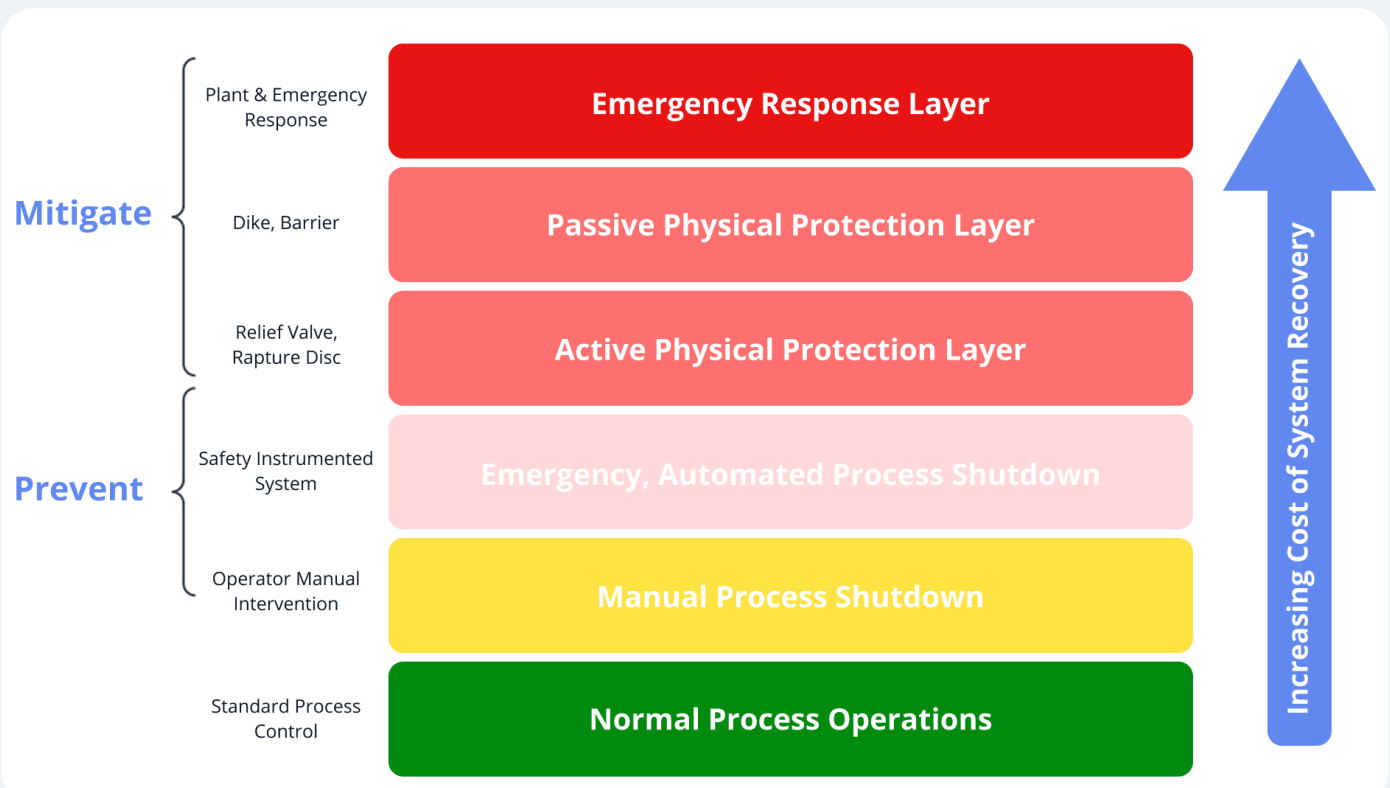


Figure 3: Layers of Process Protection in Industrial Environments

There are nonetheless significant signs of continued adversary interest in executing or preparing for integrity-targeting attack scenarios. For example, in 2022 researchers disclosed an OT-focused malware framework known alternatively as Incontroller or PIPEDREAM. This malware, identified through unspecified means prior to its actual use in a victim environment, would enable targeted interactions with specific industrial equipment and protocols that could be used for staging or enabling attack scenarios such as those described above.[34] [35] While not observed "in the wild" in terms of actual use, the very existence of Incontroller demonstrates continued adversary interest in developing (and potentially deploying) OT-aware capabilities for process-specific manipulation actions.

Even with adversary ambitions spurring the development of OT-aware payloads such as Incontroller (to say nothing of historical, but largely failed, destruction attempts), actual mission accomplishment remains elusive in integrity-targeting scenarios. A key reason for this is that physical processes, the target of adversary actions, include various safety systems and engineering controls designed specifically to avoid or dampen "worst-case" scenarios. From Safety Instrumented Systems (SIS) to "dumb" technology such as relief valves and rupture discs, as highlighted in Figure 3 above, migrating impacts from pure cyber actions to physical effects entails not just understanding but overcoming a variety of controls beyond OT manipulation. While some of these may be amenable to interference, as demonstrated in the Triton incident's attempt to manipulate a SIS,[36] others are beyond any sort of logical manipulation or subversion as they simply do not have a cyber component.

Because of the above, adversaries such as VT must devise some mechanism to evade, disable, or destroy safeguards (including physical and engineering controls) to allow for a cyber impact to propagate beyond the safety and protection layer. Options for doing so require actions ranging from malicious insiders to kinetic strikes on equipment, but all necessitate physical, direct interaction with non-cyber, non-networked controls to overcome protection mechanisms. These options would seem to make any cyber component unnecessary or irrelevant though, as willingness to engage in such direct action means simply bombing infrastructure or similar actions now appear to be within scope.

If an entity needs to drop a bomb or commit physical sabotage to allow for a cyber effect to migrate to physical process destruction, the "enabling" function for cyber can simply replace such technical actions completely. Analysts may have already witnessed this in practice in the current phase of Russia's invasion of Ukraine, where electric sector-targeting cyber operations have been dwarfed by sustained bombing campaigns against electric sector infrastructure.[37] VT's actions and ambitions may thus be questioned if direct physical damage or destruction is their assessed goal.

Where matters get more interesting is considering the possibilities of introducing latent integrity-impacting capabilities into the environment that may induce physical disruption or destruction as part of a sequence of events. We can look to the 2016 Ukraine

incident where the timing and staging of capabilities strongly suggest the adversary attempted to remove process protection (disabling Siemens SIPROTEC protective relays) anticipating an operator rush to physical process restoration, resulting in an unprotected transmission line.[38] While it remains unknown if this attack scenario would have succeeded in causing damage (as the adversary made numerous mistakes in executing the intrusion), the 2016 incident's ambition highlights interesting scenarios for OT-targeting adversaries.

Extending to VT, persistent access to a victim environment can enable a variety of potential integrity-targeting scenarios. As seen in historical events, such as what was likely intended with Triton,[39] SIS, protection, or similar systems could potentially be modified, disabled, or otherwise impacted to remove safeguards from environments allowing for other events, either directly induced by the adversary or stemming from natural process variation, to propagate beyond safety and protection layers. The former allows for effects at a time of the adversary's choosing, while the latter is less predictable. As such, analysts should assess that VT would chain intrusions in an attempt to remove safety and protection items to the greatest extent possible, then execute some process manipulation to create a physical impact scenario. This attack sequence highlights the criticality of safety and protection systems for defense, monitoring, and integrity checks as they represent a necessary item for VT to modify, disable, or otherwise interact with to achieve any type of cyber-physical outcome.

Reviewing the limited number of known integrity-targeting events, analysts may look to the only successful campaign for lessons: Stuxnet. In the Stuxnet incident, subversion of plant controls and telemetry (e.g., replaying "normal" device monitoring during attack sequences) allowed destructive capabilities to propagate beyond automated or operator intervention to achieve physical process destruction.[40] [41] As noted in analysis of Stuxnet, such an attack requires a layered intrusion consisting of both capabilities to overcome safety and protection controls (Triton's capability to allow for arbitrary interaction with SIS is also relevant in this respect), as well as the actual destructive payload.

To date, VT has not demonstrated the possession of either of these critical functions. However, given the appearance of tools such as Incontroller and VT's investment in long-running, resource-intensive intrusions, such capabilities are not beyond the reach of most state-directed, well-resourced adversaries. The ability to execute a multi-layered attack scenario requires a combination of target analysis, functional research, and capability development to properly execute. Based on publicly available information, VT has already satisfied several of these steps through its long-running intrusions in US critical infrastructure.

Any VT scenario targeting process integrity will require not just access for capability deployment, but substantial research and information collection to allow for capability development as well. Some of this appears to be taking part within broader PRC OT-nexus cyber operations, such as the extensive

investment in OT simulation and testing environments that would allow for offensive capability development.[42] Such investments could then be leveraged by VT or related actors to procure or receive a payload for physical process impact. At present, these are only assessed links and firm relationships between these programs are not established in publicly available information.

Confidentiality: Preparation & Capability Development

VT activity is strongly associated with collection of OT-related data based on multiple open source reports.[43] [44] Such activity allows for target development and attack planning (e.g., what systems or assets are necessary to target to achieve specific effects), as well as gathering system information and characteristics to ascertain what capabilities are necessary to interact with identified equipment and installations.

VT's IT-focused intrusions looking for OT-related data are concerning, but analysts can anticipate that information gathering will extend to OT environments with high degrees of confidence. Reasons for this include:

1. Enabling specific understanding of exact systems and configurations to ensure any follow-on capabilities and payloads are designed for the targeted environment.
2. Overcoming configuration and deployment "drift" from initial installation and setup (captured in source documents and other items likely housed in IT systems), where OT system and production status represents "ground truth" information on actual setup.
3. The overlap between access for gathering information and access for subsequent capability delivery, where the two almost certainly overlap to significant degrees in most environments making them complementary actions in an intrusion scenario.

PRC cyber operations have historically been viewed as largely targeting information confidentiality, with significant loss of data and intellectual property to traditional and economic espionage operations.[45] While there is much evidence behind this, discussions on VT have emphasized how the group's actions are not aligned with traditional intelligence goals and tradecraft, but instead represent the actions necessary for critical infrastructure disruption and interference.[46]

Analysts and policy makers should anticipate a lengthy and sustained information gathering campaign, including against and within OT environments, as a prerequisite for more disruptive VT operations. Moreover, such activity is likely to be continuous in nature to ensure that VT operations have the most accurate and relevant information necessary to enable subsequent cyber-physical outcomes, whether these are direct disruption events or more ambitious integrity-targeting intrusions.

Proposed Volt Typhoon Attack Scenario

At present VT appears to be in a preparatory phase for future cyber-physical operations in OT environments. While immediate disruptive operations are possible, higher impact scenarios require a combination of wider OT environment access and OT-specific capability development. Importantly, VT actions must be placed within wider strategic contexts: notably as a mechanism to impair, impede, or impose costs on US responses to a potential Taiwan Strait invasion scenario. In this respect, target selection and focus along with effect timing are critical elements guiding VT actions.

Any VT operation, given the long-running and operationally expensive intrusion operations identified over several years (even if only in terms of opportunity cost), would presumably need a return on investment to justify itself. In a Taiwan scenario, that would mean impacting US critical infrastructure and associated capabilities in a way that would materially influence this conflict. For example, either inhibiting the transportation of material to US West Coast ports and on to the Pacific region, or causing some degree of domestic pain that would serve as a deterrent toward further US involvement.

As such, an immediate, direct disruption action against IT-like assets in production environments would appear too limited in scope and duration due to options to move operations to "manual" modes or work around impacted systems. In certain specific, targeted instances, such disruption may be valuable but would represent a limited and likely short-duration impact scenario for reasons previously described. While representing the lowest barrier to entry and potentially producing value in terms of signaling or creating public concern (or panic), these outcomes are unpredictable in value and outcome making them less enticing given investments made in VT intrusions thus far.

Conversely, activity that could lead to long-term asset disabling of physical damage to key infrastructure nodes would be extremely valuable in a Taiwan scenario as it could either directly impact US force projection or impose noticeable costs on US economic activity. While substantially more difficult to execute, the return on investment in greater in terms of effects, both direct (damage inflicted) and indirect (inducing panic and potentially decision paralysis). US responses to such a significant action would also likely be more forceful, creating escalation concerns, but could come from a substantially weaker position than before a VT attack scenario given uncertainty as to the integrity of critical systems and what additional actions may be possible on the part of VT or other PRC-linked entities.

Based on the above evaluations, an integrity-targeting scenario as outlined in previous sections appears to be the most impactful and likely scenario for a VT cyber-physical operation of any significance. Direct availability actions may take place simultaneously but would be operationally less impactful and more easily mitigated. Yet done in tandem with more critical attacks on fundamental system operations, VT could create conditions of public and economic chaos.

Given available public information, VT does not appear to possess the combination of access and capabilities to execute such a disruptive event in the immediate term. While the group has successfully penetrated critical networks associated with military operations, such as entities in Guam,[47] these efforts take place alongside seemingly irrelevant operations such as intrusions into the Littleton Electric Light and Water Departments.[48] Thus available information may indicate a lack of focus or a highly opportunistic nature to VT operations that may dull its ability to execute truly concerning attack scenarios.

Significant uncertainty therefore remains in terms of VT actions, but if assessments from US officials as to VT's intentions or tasking are reasonably accurate,[49] the potential for significant impacts mean caution is required. As a result, analysts and infrastructure owners and defenders can, based on the above analysis of both VT actions and historical OT-targeting capabilities, plan for a scenario similar to the following:

1. VT leverages captured credentials and similar authentication or identity information to access or move laterally within OT environments.
2. VT extracts process and technical information from targeted OT environments for target and capability development.
3. Leveraging the same access developed in #2, VT can seed relevant capabilities, even if only backdoors or the ability to continuously gather new or changed authentication information, in victim environments to ensure sustained, persistent access.
4. When the desired time comes for a transition from collection to action, VT can leverage existing access points and mechanisms from #2 and #3 to push capabilities developed through information gathering in #2 to victim environments, starting with actions to defeat or degrade safety and protection mechanisms.
5. Satisfying #4, VT can then deploy disruptive or destructive payloads in victim OT environments, or engage in process manipulation, with the intent that these propagate beyond now degraded safety and protection mechanism to achieve a cyber-physical effect.

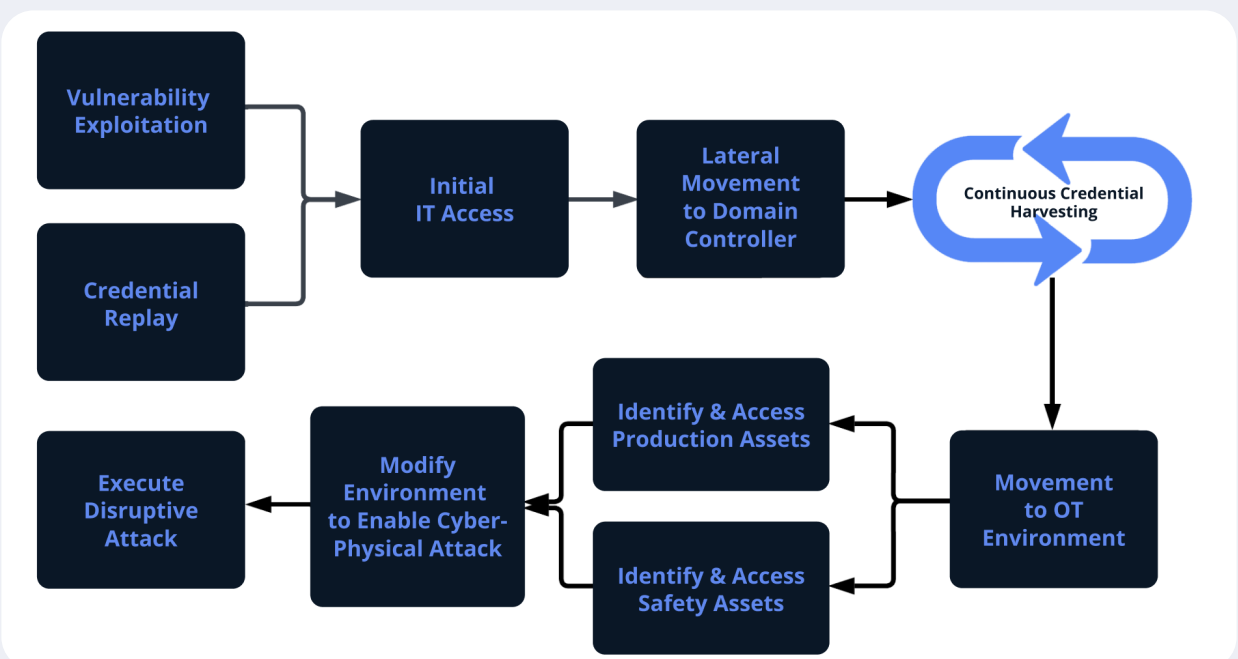


Figure 4: Volt Typhoon Attack Scenario

This scenario is deeply concerning in that it would result in at minimum process disruption, if not physical destruction including long-term downtime or even (immediate or follow-on) loss of life. Yet this scenario is also exceptionally difficult to achieve, especially at a scale that extends from a single victim to many entities that would be necessary for economy-wide impact scenarios. As a result, VT, should it go "active" (or pass on its access to another entity to engage in a disruptive effect), will find itself with a challenge of going "deep" into some, highly valuable environments (targeting them for tailored disruptive or destructive operations), or "wide" into many environments roughly simultaneously but to a lesser degree of disruption.

While incomplete and lacking desired information, the above assessment remains valuable for focused decision-making among policy makers, asset owners, and network defenders in a contested operating environment. For example, by dispensing with the notion that VT is somehow invincible and can disrupt (or destroy) any critical infrastructure at any time, we can recognize the limitations and costs associated with the group's operations. These costs and bounds can then inform defense and response through identifying the adversary's own "pain points" in mission accomplishment.

Mitigatons & Responses

VT and similar entities operate in a way explicitly designed to evade legacy security controls and alerting. However, multiple options exist to disadvantage or outright eliminate Volt Typhoon behaviors, removing entire categories of intrusion tradecraft from adversary operations.

The first and foremost item of concern in defending against a VT operation is the security and confidentiality of user authentication information. VT, along with other threat actors, such as the prolific criminal group Scattered Spider, thrive on the subversion of legitimate user credentials to facilitate operations, Building robust systems that incorporate multifactor authentication (MFA) and regular auditing, especially when concerning authentication to sensitive systems (domain controllers) or critical networks (OT environments), can severely limit the possibilities of a VT-like intrusion.

In concert with the above, visibility and monitoring of authentication information is critical in tracking adversaries such as VT. Particularly in an era where authentication and permission information is handled in third-party and cloud environments, understanding where logs and related information reside and how to query them is critical to maintain visibility and understanding of intrusion pathways. Building the capacity today around single sign-on (SSO) and identity access management (IAM) solutions for monitoring and security is necessary to track the evolution of threat actors like VT as they find system-specific authentication more difficult to subvert.

Fior cyber-physical targeting entities such as VT, identifying mechanisms to trigger when adversaries access sensitive networks is critical. Much of this pertains to defense-minded architectural decisions, such as limiting access to OT environments or enabling access only through dedicated, monitored "jump hosts." Establishing a robust, limited,

and environment that constrains adversary actions both diminishes adversary operations while enhancing opportunities for detection and discovery.

Finally, organizations must maintain awareness of operations such as VT to inform security and policy decision making in near real-time. Ignorance of operations such as VT intrusions dooms organizations to less than optimal decisions in resource-limited environments. Understanding how campaigns and threat actors such as VT operate, what they are targeting, and their likely intentions are critical data points to inform security decisions to enable more robust, relevant defensive responses.

Conclusion

VT actions represent the most direct and acute threat to US critical infrastructure operations at present. However, such operations do not take place in a technical or strategic vacuum. We should anticipate VT operations shifting from the present course of intrusion, persistence, and information extraction to more direct operations aligned with higher-level interests and concerns, such as those involving a Taiwan Strait crisis. As such, VT represents a significant but nascent threat, not necessarily an immediate one given broader strategic concerns and operational "triggers" for more aggressive actions. Even absent an immediate threat though, the degree to which VT has accessed and probed environments of interest remains a concern.

VT is a dangerous actor that is rapidly moving towards a position where it can legitimately and credibly place critical infrastructure assets at risk. However, it is important to note the significant barriers, in terms of not just IT and OT defenses but also physical and engineering controls, that VT must overcome to achieve its most concerning potential outcomes.

Given the above, significant opportunities exist for asset owners and defenders such as expanding visibility into monitored environments and emphasizing operational resiliency to defeat VT (or other) attack scenarios. While building greater resilience and the capability to defeat VT are neither cheap nor easy, an increasingly contested critical infrastructure space demands that owners and defenders rapidly pivot to defend against or degrade the capabilities of such actors. Failure to do so leaves entities such as VT with the time necessary to build points of presence within victim environments and develop the capabilities necessary to harm them as well.

Understanding VT operations is vital to defense and response, but understanding how a likely VT cyber-physical action would take place is equally important. Understanding the capabilities of a VT while also acknowledging the limitations on such actors due to physical process controls is necessary to appropriately scoping the threat. By understanding these items, analysts and policy makers can hopefully direct resources in the most effective and efficient way to defeat these adversaries, while also ensuring operational resilience and service continuity for potential victims.

Sources

[1] J. Lyons, "This is the FBI, open up. China's Volt Typhoon is on your network," The Register, 12 March 2025. [Online]. Available: https://www.theregister.com/2025/03/12/volt_tyhoon_experience_interview_with_gm/. [Accessed 12 July 2025].

[2] US Cybersecurity & Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," US Cybersecurity & Infrastructure Security Agency, 07 February 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. [Accessed 12 July 2025].

[3] J. Slowik, "VB2018 paper: Anatomy of an attack: detecting and defeating CRASHOVERRIDE," Virus Bulletin, 2018. [Online]. Available: https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/. [Accessed 12 July 2025].

[4] US Cybersecurity & Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," US Cybersecurity & Infrastructure Security Agency, 07 February 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. [Accessed 12 July 2025].

[5] Microsoft Threat Intelligence, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," Microsoft, 24 May 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/. [Accessed 12 July 2025].

[6] Counter Threat Research Team, "Chinese Cyberespionage Group Bronze Silhouette Targets U.S. Government and Defense Organizations," Secureworks, 24 May 2023. [Online]. Available: https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations. [Accessed 12 July 2025].

[7] J. Slowik, "Evolution of ICS Attacks and the Prospects for Future Disruptive Events," Dragos, 2018. [Online]. Available: https://www.dragos.com/wp-content/uploads/Evolution-of-ICS-Attacks-and-the-Prospects-for-Future-Disruptive-Events-Joseph-Slowik-1.pdf. [Accessed 12 July 2025].

[8] J. Slowik, "VB2018 paper: Anatomy of an attack: detecting and defeating CRASHOVERRIDE," Virus Bulletin, 2018. [Online]. Available: https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/. [Accessed 12 July 2025].

[9] US Cybersecurity & Infrastructure Security Agency, "Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors," US Cybersecurity & Infrastructure Security Agency, 15 March 2018. [Online]. Available: https://www.cisa.gov/news-events/alerts/2017/10/20/advanced-persistent-threat-activity-targeting-energy-and-other-critical-infrastructure-sectors. [Accessed 12 July 2025].

[10] J. Slowik, "The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure," Virus Bulletin, October 2021. [Online]. Available: https://vblocalhost.com/uploads/VB2021-Slowik.pdf. [Accessed 12 July 2025].

[11] M. Raggi, "IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders," Google Cloud, 22 May 2024. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks. [Accessed 12 July 2025].

[12] Black Lotus Labs, "Routers Roasting On An Open Firewall: The KV-Botnet Investigation," Lumen, 13 December 2023. [Online]. Available: https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/. [Accessed 12 July 2025].

[13] US Department of Justice, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure," US Department of Justice, 31 January 2024. [Online]. Available: https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical. [Accessed 12 July 2025].

[14] Black Lotus Labs, "KV-Botnet: Don't Call It A Comeback," Lumen, 07 February 2024. [Online]. Available: https://blog.lumen.com/kv-botnet-dont-call-it-a-comeback/. [Accessed 12 July 2025].

[15] M. J. Assante and R. M. Lee, "The Industrial Control System Cyber Kill Chain," SANS, 05 October 2015. [Online]. Available: https://www.sans.org/white-papers/36297/. [Accessed 12 July 2025].

[16] US Cybersecurity & Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," US Cybersecurity & Infrastructure Security Agency, 07 February 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. [Accessed 12 July 2025].

[17] Microsoft Threat Intelligence, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," Microsoft, 24 May 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/. [Accessed 12 July 2025].

[18] J. Lyons, "This is the FBI, open up. China's Volt Typhoon is on your network," The Register, 12 March 2025. [Online]. Available: https://www.theregister.com/2025/03/12/volt_tyhoon_experience_interview_with_gm/. [Accessed 12 July 2025].

[19] J. Hanrahan, "VOLTZITE Espionage Operations Targeting U.S. Critical Systems," Dragos, February 2024. [Online]. Available: https://hub.dragos.com/hubfs/116-Datasheets/Dragos_SB_IntelVOLTZITE_Feb24_FINAL_r4.pdf. [Accessed 12 July 2025].

[20] R. Satter, Z. Siddiqui and J. Pearson, "U.S. warns China could hack infrastructure, including pipelines, rail systems," Reuters, 26 May 2023. [Online]. Available: https://www.reuters.com/world/china/china-rejects-claim-it-is-spying-western-critical-infrastructure-2023-05-25/. [Accessed 12 July 2025].

[21] Z. Siddiqui, "US confronts China over Volt Typhoon cyber espionage," Reuters, 08 May 2024. [Online]. Available: https://www.reuters.com/world/us/us-confronts-china-over-volt-typhoon-cyber-espionage-2024-05-08/. [Accessed 12 July 2025].

[22] Electricity Information Sharing and Analysis Center, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 18 March 2016. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf. [Accessed 12 July 2025].

[23] N. Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," The New York Times, 24 October 2012. [Online]. Available: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html. [Accessed 12 July 2025].

[24] Threat Hunter Team, "Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail," Symantec, 14 Deceber 2018. [Online]. Available: https://www.security.com/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail. [Accessed 12 July 2025].

[25] Booz Allen Hamilton, "When the Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure," September 2016. [Online]. Available: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf. [Accessed 12 July 2025].

[26] A. Cherepanov, "WIN32/Industroyer: A new threat for industrial control systems," ESET, 12 June 2017. [Online]. Available: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf. [Accessed 12 July 2025].
[27] ESET Research, "Industroyer2: Industroyer Reloaded," ESET, 12 April 2022. [Online]. Available: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/. [Accessed 12 July 2025].
[28] J. Slowik, "VB2018 paper: Anatomy of an attack: detecting and defeating CRASHOVERRIDE," Virus Bulletin, 2018. [Online]. Available: https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/. [Accessed 12 July 2025].
[29] A. Cherepanov, "WIN32/Industroyer: A new threat for industrial control systems," ESET, 12 June 2017. [Online]. Available: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf. [Accessed 12 July 2025].
[30] Electricity Information Sharing and Analysis Center, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 18 March 2016. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf. [Accessed 12 July 2025].
[31] J. A. Guerrero-Saade and M. van Amerongen, "AcidRain | A Modem WIper Rains Down on Europe," SentinelLabs, 31 March 2022. [Online]. Available: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/. [Accessed 12 July 2025].
[32] J. A. Guerrero-Saade and T. Hegel, "AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine," SentinelLabs, 21 March 2024. [Online]. Available: https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/. [Accessed 12 July 2025].
[33] J. Slowik, "Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on Industrial Environments," Dragos, 2019. [Online]. Available: https://www.dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf. [Accessed 12 July 2025].
[34] N. Brubaker, K. Lunden, K. Proska, M. Umair, D. K. Zafra, C. Hildebrandt and R. Caldwell, "INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems," Google Cloud, 13 April 2022. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/incontroller-state-sponsored-ics-tool. [Accessed 12 July 2025].
[35] Dragos, "PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems," Dragos, 2022. [Online]. Available: https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf. [Accessed 12 July 2025].
[36] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker and C. Glyer, "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure," Google Cloud, 14 December 2017. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/attackers-deploy-new-ics-attack-framework-triton. [Accessed 12 July 2025].
[37] T. Vatman and C. Hart, "Russia's attacks on Ukraine's energy sector have escalated again as winter sets in," International Energy Agency, 17 January 2024. [Online]. Available: https://www.iea.org/commentaries/russias-attacks-on-ukraines-energy-sector-have-escalated-again-as-winter-sets-in. [Accessed 12 July 2025].
[38] J. Slowik, "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack," Dragos, 2018. [Online]. Available: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf. [Accessed 12 July 2025].
[39] J. Slowik, "Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on Industrial Environments," Dragos, 2019. [Online]. Available: https://www.dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf. [Accessed 12 July 2025].
[40] J. Slowik, "Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on Industrial Environments," Dragos, 2019. [Online]. Available: https://www.dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf. [Accessed 12 July 2025].
[41] K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York: Penguin Random House, 2014.
[42] D. Cary, "Downrange: A Survey of China's Cyber Ranges," Georgetown Center for Security and Emerging Technology, September 2022. [Online]. Available: https://cset.georgetown.edu/wp-content/uploads/CSET-Downrange-A-Survey-of-Chinas-Cyber-Ranges-1.pdf. [Accessed 12 July 2025].
[43] . Lyons, "This is the FBI, open up. China's Volt Typhoon is on your network," The Register, 12 March 2025. [Online]. Available: https://www.theregister.com/2025/03/12/volt_tyhoon_experience_interview_with_gm/. [Accessed 12 July 2025].
[44] J. Hanrahan, "VOLTZITE Espionage Operations Targeting U.S. Critical Systems," Dragos, February 2024. [Online]. Available: https://hub.dragos.com/hubfs/116-Datasheets/Dragos_SB_IntelVOLTZITE_Feb24_FINAL_r4.pdf. [Accessed 12 July 2025].
[45] B. Jensen, "How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy," Center for Strategic & International Studies, 19 October 2023. [Online]. Available: https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy. [Accessed 12 July 2025].
[46] US Federal Bureau of Investigation, "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says," US Federal Bureau of Investigation, 18 April 2024. [Online]. Available: https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says. [Accessed 12 July 2025].
[47] Microsoft Threat Intelligence, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," Microsoft, 24 May 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/. [Accessed 12 July 2025].
[48] J. Lyons, "This is the FBI, open up. China's Volt Typhoon is on your network," The Register, 12 March 2025. [Online]. Available: https://www.theregister.com/2025/03/12/volt_tyhoon_experience_interview_with_gm/. [Accessed 12 July 2025].
[49] US Federal Bureau of Investigation, "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says," US Federal Bureau of Investigation, 18 April 2024. [Online]. Available: https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says. [Accessed 12 July 2025].