Past Cyber Operations Against Ukraine and What May Be Next

crowdstrike.com/blog/lessons-from-past-cyber-operations-against-ukraine/

CrowdStrike Intelligence Team

January 28, 2022

Disruptive and destructive cyber operations have been levied against elements of Ukrainian society by adversaries attributed to the Russian government — or groups highly likely to be controlled by them — since at least 2014. These operations have impacted several sectors, including energy, transportation and state finance, and have attempted to influence political processes and affect businesses more broadly within the country.

These operations have been conducted in a semi-deniable manner, providing enough evidence to arouse suspicion of the likely perpetrators — so as to ensure that intended messaging is conveyed to targeted entities — while also obfuscating the activity's origins. CrowdStrike attributes the majority of the known offensive operations against Ukraine to VOODOO BEAR, an adversary highly likely controlled by the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

The impact of offensive operations is rarely constrained to the initial target entity, with collateral damage occurring either directly through corruption of computer networks or indirectly through interruption of critical business services on which organizations rely for day-to-day operation. Analysis of previous activities has identified several situations in which apparently localized targeting has caused unintended consequences to organizations outside of Ukraine.

This blog will evaluate major disruptive events against Ukrainian interests in the past and attempt to forecast likely forms and outcomes of future operations within the region.

Detail

Techniques employed by VOODOO BEAR to facilitate and deliver destructive effects have evolved over the years, from the distribution of targeted wiper malware via custom loaders to mimicking the effect of ransomware deployments using wider-reaching distribution mechanisms such as supply chain and strategic web compromises (SWC).

However, the pretense of ransomware is often superficial and its implementation is not consistent with financially motivated criminal actors. There is also evidence to suggest that the adversary has leveraged attribution fronts claiming to be motivated by hacktivist ideologies alongside destructive campaigns, likely in an attempt to amplify the effects of the attacks by publicizing them more widely.

CrowdStrike Intelligence has reported extensively on VOODOO BEAR operations within Ukraine, with overviews of their evolving operations available to our premium intelligence subscribers. These campaigns are assessed to likely contribute to psychological operations seeking to degrade, delegitimize or otherwise influence public trust in state institutions and industry sectors in the country.

2014-2016: Targeted Attacks Using Custom Delivery Malware

Early destructive operations attributed to VOODOO BEAR have targeted a range of sectors within Ukraine, often leveraging a combination of the *BlackEnergy* malware (version 3) and the *KillDisk* (aka *PassKillDisk*) wiper. Many campaigns were timed to coincide with specific events or seasons, while the events in December 2016 could be interpreted as a persistent execution of successive attacks designed to have a multiplicative disruptive effect on the country.

These operations included:

- May 2014: targeting of energy and transportation organizations
- October 2015: targeting of media outlets, coinciding with local elections
- December 2015: targeting of an energy provider in western Ukraine
- December 2016: targeting of state-operated financial institutions (FIs) and rail companies
- December 2016: targeting of an energy provider causing power outages in Kiev
- December 2016: targeting of the Ukrainian State Hydrographic Service

Despite the relatively focused targeting in each of these cases, variants of the *KillDisk* malware distributed in December 2016 were modified to mimic ransomware and hacktivist intent, foreshadowing later developments in operational tactics, techniques and procedures (TTPs).

Observations of contemporary activity in this period suggest that attribution fronts adopting hacktivist personas were used to publicly release data from Ukrainian organizations alongside these offensive operations, although the exact nature of their coordination is unclear. For example, the CyberBerkut collective claimed responsibility for destructive and denial-of-service (DoS) attacks against the Ukrainian Central Election Commission (CEC) in May 2014, after which the group began publishing sensitive emails and internal documents from the CEC to support their claim.

Similarly, in December 2016, a pro-Russia hacktivist group called Sprut leaked a series of documents related to the finances of the Ukrainian government's state energy company. Later that month, the group announced they had disrupted the main website of the Ukrainian Energy company Ukrenergo, which had publicly acknowledged that internal systems had been accessed on Dec. 17-18, 2016. Information operations (IO) combining public (disruptive) and non-public (destructive) intent are highly likely representative of attempts to amplify the effects of damage to government systems by controlling public narrative over an extended period.

2016-2017: Increased Deniability and Scale Through the Use of Pseudo-Ransomware

VOODOO BEAR's destructive operations in 2017 marked a distinct change in deployment and destructive payload TTPs. Building on earlier attempts to masquerade wipers as criminal ransomware, several campaigns using different — but technically linked — pseudo-ransomware families were deployed by the adversary against Ukrainian entities.

Of particular note was the adoption of several deployment techniques that greatly amplified the potential scope and destructive implications of these operations. The use of supply chain compromise and SWC methodologies vastly increased the number of victims impacted by each campaign, and worm-like propagation mechanisms supported by the *Mimikatz* credential-stealing tool and the EternalBlue exploit for the CVE-2017-0144 vulnerability increased the potential impact on networks after initial infection.

These operations included:

- January 2017: *Filecoder.NKH* was deployed via a supply chain compromise of a Ukrainian IT company
- May 2017: *XDATA* was deployed for a short period via the software update mechanism of M.E. Doc, a Ukrainian accounting software product used by many companies either located — or operating — within Ukraine

- June 2017: *FakeCry* also was deployed via a malicious M.E. Doc update, a malware family impersonating the infamous WannaCry ransomware
- June 2017: *NotPetya* was deployed via the same M.E. Doc mechanism, with earlier tests likely deployed via SWC of a Ukrainian media website
- October 2017: *BadRabbit* was deployed against Ukrainian transport networks via SWC of websites in several countries including Ukraine, Russia, Turkey and Bulgaria

Observations of a phased approach to the distribution of pseudo-ransomware variants across multiple delivery vectors suggest that campaigns in early 2017 may have been tests for the wider distribution of *NotPetya*, which was apparently timed to coincide with Ukraine's Constitution Day. However, distribution of *NotPetya* via the M.E. Doc update mechanism — also used by non-Ukrainian organizations — and the implementation of unconstrained propagation techniques resulted in global spread with likely unintended impact to a wide variety of sectors including logistics, healthcare and retail. The *BadRabbit* campaign also appeared to have resulted in collateral damage against some Russia-based organizations, likely as a result of victims visiting websites used to distribute the malware.

2022: Hybrid Operations Using Multiple Campaign Stages

January 2022 reporting on what CrowdStrike tracks as the WhisperedDebate activity cluster involving website defacements and *WhisperGate* wiper operations against Ukrainian government networks demonstrates the continued intent to disrupt state institutions. CrowdStrike Intelligence does not currently attribute WhisperedDebate to a named adversary (e.g., VOODOO BEAR), although high-level parallels to previous operations, the Ukrainian focus and timing of the activity strongly suggest a Russia-nexus adversary or a group aligned with their interests.

Public statements from the Ukrainian government suggest that the scope of this operation was relatively constrained compared to VOODOO BEAR campaigns in 2017, although it is unknown whether this was intentional or representative of operational difficulties experienced by the adversary. However, the likely manual malware distribution vector employed and the focus on targeting of government networks — and other destructive attacks against IT service providers, likely in an attempt to cover up evidence of initial intrusion vectors — indicates that limited impact was intentional in this case.

CrowdStrike has identified several attempts to distribute data purportedly acquired from several government organizations shortly after they had been targeted during the WhisperedDebate campaign, supporting claims made in the website defacement messages. While links between these events have not been conclusively proven at the time of writing, data leak evidence presented by several personas presenting hacktivist or criminal motivations may be representative of an attempt to execute an IO campaign to successively release personally identifiable information (PII), contrary to repeated statements from

Ukrainian officials that no data had been taken during the network intrusions. These attempts can seek to degrade public trust in the government's ability to effectively address the breaches.

This use of IO mirrors earlier VOODOO BEAR TTPs, where the *CyberBerkut* and *Sprut* group personas contemporaneously released private data from Ukrainian organizations. The introduction of publicly visible website defacements during the WhisperedDebate activity provides an additional facet to the operation that can be easily picked up and amplified by media outlets.

Assessment

The extended history of destructive VOODOO BEAR operations against Ukrainian entities indicates a commitment to the execution of psychological operations against the local populace. This represents ongoing Russian government efforts to influence Ukraine against a backdrop of national security and populist policies.

Ultimately, these operations and their intended effects are complementary to the Russian government's overall strategy pertaining to Ukraine, although they do not appear to be specifically linked to overt diplomatic efforts or military maneuvers, and instead are likely intended as a separate tool that can be used to selectively increase tension within Ukraine and destabilize public trust in Ukrainian government institutions. The precise endgame for these actions is unclear, although coercing the population to reject closer ties with the West, establishing new leadership more favorable to Russia or preparing for military action similar to the 2014 annexation of Crimea are all possible intended outcomes.

CrowdStrike anticipates that future offensive operations against Ukraine will most likely take the form of destructive wiping attacks masquerading as ransomware. This assessment is made with moderate confidence, based on a successive evolution of technical TTPs and the acknowledgement that this type of operation can have the desired disruptive effect and signal deeper intent, while still avoiding taking direct responsibility for the attacks.

The contemporaneous use of IO campaigns to launder and publicize PII or other sensitive data stolen during network breaches and draw media awareness through website defacement activity is also likely to occur as part of hybrid operations in the future. A low chance of DoS attacks may be present in future campaigns, although this technique has not been observed in recent years and arguably has little lasting effect on targeted organizations. DoS would most likely be used in combination with other offensive actions such as wiping attacks, or to bolster credentials within hacktivist communities.

Based on observations of past events such as the spread of *NotPetya,* disruptive and destructive attacks against Ukraine are likely to have broader implications, including potential impacts to organizations based outside the country. Collateral damage is particularly likely to be experienced by companies that operate subsidiaries within Ukraine or possess network assets interconnected with Ukrainian organizations. This assessment is made with moderate confidence, although there is evidence to suggest that subsequent operations have attempted to limit the scope of unconstrained malware propagation, likely due to the significant unintended fallout of *NotPetya.* Outside of being directly impacted by destructive attacks, organizations relying on Ukrainian logistics networks are likely to experience disruptive effects of any future operations targeting part of the Ukrainian transport sector.

Destructive attacks intentionally targeted at organizations outside the country — such as those headquartered within countries supportive of Ukraine's position against Russia, including the U.S. and those in Europe — cannot be completely discounted, although this is assessed as an unlikely scenario due to the risk of uncontrolled escalation of international tension and punitive measures, including direct retaliatory actions by other governments. However, the incidental targeting of international businesses operating within Ukraine may be used by Russian-nexus adversaries to dissuade business operations and investment and destabilize the local economy.

CrowdStrike Intelligence Confidence Assessment

High Confidence: Judgments are based on high-quality information from multiple sources. High confidence in the quality and quantity of source information supporting a judgment does not imply that that assessment is an absolute certainty or fact. The judgment still has a marginal probability of being inaccurate.

Moderate Confidence: Judgments are based on information that is credibly sourced and plausible, but not of sufficient quantity or corroborated sufficiently to warrant a higher level of confidence. This level of confidence is used to express that judgments carry an increased probability of being incorrect until more information is available or corroborated.

Low Confidence: Judgments are made where the credibility of the source is uncertain, the information is too fragmented or poorly corroborated enough to make solid analytic inferences, or the reliability of the source is untested. Further information is needed for corroboration of the information or to fill known intelligence gaps.

Additional Resources

- *Find out how to stop adversaries targeting your industry — schedule a free 1:1 intel briefing with a CrowdStrike threat intelligence expert today.*
- *Learn how Falcon X™ Premium cyber threat intelligence enables your security teams to become intelligence-led by exposing the adversaries and evolving tradecraft targeting your business.*
- *Learn about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ to see for yourself how true next-gen AV performs against today's most sophisticated threats.*