



VB2021
localhost

7 - 8 October, 2021 / vblocalhost.com

THE BAFFLING BERSERK BEAR: A DECADE'S ACTIVITY TARGETING CRITICAL INFRASTRUCTURE

Joe Slowik

Gigamon, USA

joe.slowik@gigamon.com

ABSTRACT

Berserk Bear, alternatively referred to as Dragonfly, Crouching Yeti, and several other names, has compromised multiple networks across several continents since at least 2010. In that time, Berserk Bear infiltrated numerous industrial and critical infrastructure entities – but with no known, deliberate disruptive effect. In this sense, Berserk stands apart from other entities targeting critical infrastructure linked to Russian intelligence organizations, such as Sandworm, which induced multiple disruptions in various entities over the same period.

Berserk thus appears a curious entity: capable of leveraging various sophisticated techniques, such as vendor and supply chain intrusions, to breach some of the most sensitive civilian institutions in Europe and North America, while seemingly doing nothing with such access. Yet for all its lack of direct impact such activity is not benign, and likely does not represent mere information gathering. Rather, Berserk’s actions represent long-term capability and access development designed to prepare for action in the most frightening of environments: outright conflict between Berserk’s sponsors or directors (likely Russian strategic leadership) and various Western interests.

In this paper we will explore Berserk Bear’s decade of operations, including an overview of technical capabilities and efforts, to understand this enigmatic threat actor. While doing so, we will uncover items previously linked to this group’s activity and also disclose likely physical disruption operations caused by this group accidentally, resulting in significant damage to victim environments. As a result of this discussion, we will not only learn more about a particularly interesting threat actor, we will also discover vital aspects concerning supply chain intrusions, cyber contributions to preparation for kinetic warfare, and what happens when intrusions in cyber-physical environments produce unintended results.

INTRODUCTION

‘Berserk Bear’ refers to a cyber threat actor operating, in various ways, since at least 2010. Alternatively referred to as Dragonfly, Energetic Bear, TEMP.Isotope, Crouching Yeti, ALLANITE or DYMALLOY, among other names [1, 2], the group launched a series of campaigns against various critical infrastructure entities, largely in Europe and North America, but is not associated with any known deliberate destructive event [3]. For the sake of simplicity, this entity will be referred to as ‘Berserk Bear’ or just ‘Berserk’ for the remainder of this paper. Linked to Russian intelligence operations by several governments and commercial researchers, Berserk Bear differentiates itself from other critical infrastructure targeting groups with similar affiliation, such as Sandworm [4], due to this lack of identified impacts.

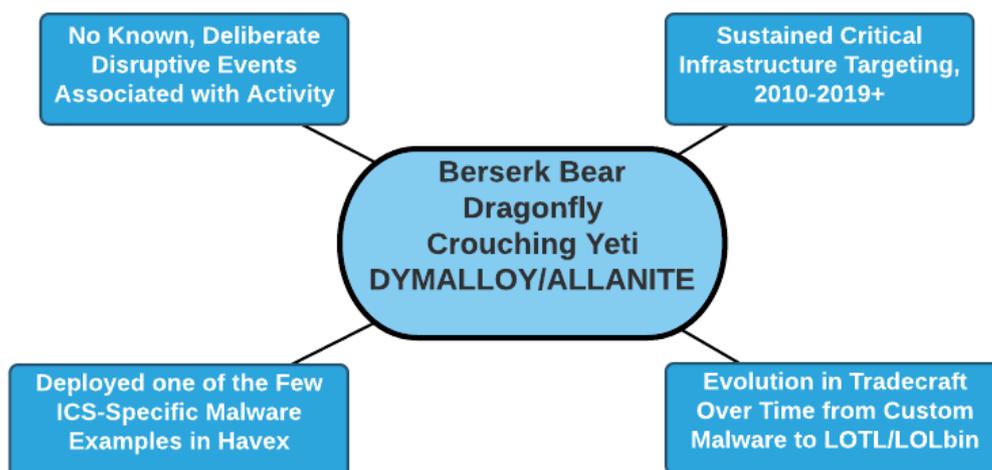


Figure 1: Berserk overview.

Yet a closer examination of Berserk Bear’s actions taking place over a decade reveals a much more nuanced and concerning picture. Although not associated with deliberate disruption, the group has targeted and successfully penetrated networks ranging from critical industrial environments to election-related operations. This continued willingness to target and breach sensitive, critical networks places Berserk in an interesting position: not pursuing immediate payoffs, but rather establishing the information collection and access development operations that could facilitate future actions at a time of its sponsor’s choosing. Given this history, a thorough review of activity linked to or associated with Berserk Bear is incredibly valuable both to understand the intentions of a worrisome adversary and to ensure awareness for defenders and policymakers.

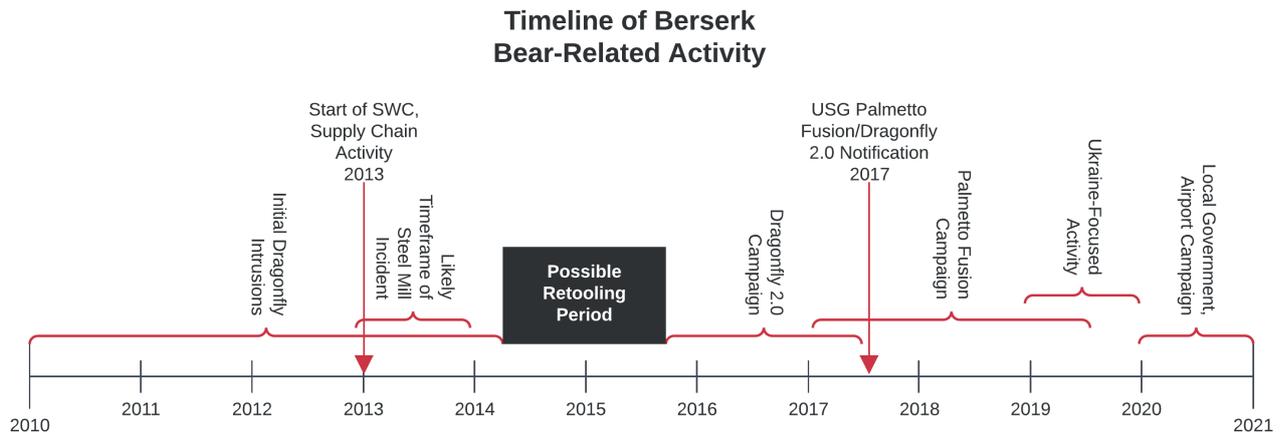


Figure 2: Berserk timeline.

THE DRAGONFLY CAMPAIGN

Berserk Bear first entered public consciousness through public reporting from *Symantec*, *Kaspersky* and *CrowdStrike* (who then referred to the entity as Energetic Bear) [5, 6, 7]. Piecing together observations from each vendor, we witness a widespread campaign starting no later than 2010 (but possibly earlier) through at least 2014, targeting manufacturing, oil and gas, and electric utility entities across North America and Europe. On a technical level, this activity is notable for blending operational techniques. At various times, Berserk Bear utilized mechanisms ranging from traditional phishing to strategic website compromise (SWC), to supply chain intrusions for initial access. In most cases, such operations led to the deployment of actor-specific malware, notably (but not exclusively) the modular Havex family.

Phishing activity

Throughout its initial period of activity, Berserk leveraged phishing with malicious attachments as a primary component of initial access operations [6]. In all documented cases, which were active in 2013–2014 but also potentially as early as 2010, malicious emails were sent to various executives and senior employees at target companies. While multiple vendor reports indicate phishing messages originated from the same *Gmail* account, it is unclear if this is definitive or instead an artifact of limited visibility.

Irrespective of vector, the phishing activity consistently leveraged the same vulnerability for initial code execution: CVE-2011-0611, relating to embedded Flash objects in file formats such as *Adobe* Portable Document Format (PDF) items [5, 8, 9]. In addition to native PDFs, some vendor reporting also indicates distribution via XML Data Package (XDP) files, with a malicious PDF stored within the container [6]. In either case, typical infection activity combined the exploit (for code execution purposes), malware (typically Havex, discussed in greater detail below), and a Java archive (JAR) file used to load and execute the malware payload.

Analysing publicly and commercially available samples, attachments to malicious emails typically displayed gibberish or no substantive content, rather than a fully developed lure or decoy. This aspect of lure documents would change significantly with Berserk evolution, even if other characteristics of malicious document use would remain similar.

Strategic website compromise

Berserk employed SWC (also referred to as ‘watering hole attacks’) concurrently with phishing activity. While reporting from *Symantec* indicates SWC activity took place largely in mid- to late-2013, *Kaspersky* analysis indicates such activity may have started significantly earlier and continued through 2014. Berserk compromised a variety of websites, ranging from the energy to financial sectors, to insert a redirect to another compromised, legitimate website hosting an exploit kit [5, 10]. Overall, initial modified websites trended toward industrial, oil and gas, and electrical entities based on reporting from multiple entities. An overview of compromised sites noted in public reporting can be found in Table 1.

Initially, Berserk operations used the LightsOut exploit kit to compromise either Java or *Internet Explorer* to gain initial code execution on victim machines [10, 11]. The group then modified operations to a newer variant of LightsOut, dubbed ‘Hello’ or ‘HelloEK’ [5, 12, 13]. In all publicly identified cases, the exploit kits were used to download a payload: either a variant of Havex or a malware referred to as Karagany.

Website	Description
39essex[.]com	Legal organization operating in UK, SG and MY.
Bsicomputer[.]com	CA-located computer and server manufacturer.
Chariotoilandgas[.]com	Oil exploration and services company.
Energo-prof[.]ge	GE-based electric generation and transmission company.
Energyplatform[.]eu	European renewable energy generation consortium, no longer active.
Firstenergy[.]com	US-based electric utility.
Gamyba[.]le[.]lt	Electric generation entity in LT.
Gritech[.]fr	FR-based engineering consultancy.
Gse[.]com[.]ge	National electric system operator for GE.
Jfaerospace[.]com	US-based engineering consultancy.
Longreachoilandgas[.]com	Oil and gas exploration company.
Nahoonservices[.]com	e-Commerce services company, no longer active.
Rare[.]fr	FR-based environmental and energy consortium.
Samashmusic[.]com	Music equipment retailer.
Sbmania[.]net	SpongeBob Squarepants fan site.
Strainstall[.]com	Engineering and offshore oil and gas services company.
Utilico[.]co[.]uk	UK-based investment trust, no longer active.
Vitogaz[.]com	FR-based gas distribution company.
Vitoreseau[.]com	FR-based gas and propane distribution company.
Yell[.]ge	GE-focused business directory.

Table 1: Overview of compromised sites noted in public reporting.

Supply chain intrusions

Finally, early Berserk-related activity utilized a third intrusion mechanism: modifying installation packages for specific control system software to deliver Havex variants. In many respects the most interesting as well as the most concerning intrusion vector, this methodology relied on first breaching a given vendor or supplier of equipment (and software) for industrial environments, producing a modified installation package including malicious functionality, then replacing legitimate packages on vendor websites for ultimate victims to download.

This phase of operations is the most explicit in industrial control system (ICS)-specific targeting. As documented by Erik Hjelmvik, Joel Langill, Dale Peterson, and others, Berserk activity included at least six software suites across three vendors [14, 15, 16]:

- *MESA Imaging Swiss Ranger* photography software [17].
- *eWon Talk2M eCatcher* industrial maintenance software [18].
- *eWon eGrabit* VPN client software [19].
- Various *MB ConnectLine* tools, including *mbCONFTOOL*, *mbCHECK* and *VCOM_LAN2*, all associated with configuration software for industrial networking appliances [20].

In each of the above cases, the victim organization represented a niche supplier often integrated into larger projects, or at minimum far smaller than major ICS-related original equipment manufacturers (OEMs). Of note, although the intrusion at *MESA* is unclear (and the company has since gone out of business), both *eWon* and *MB Connect* statements indicate initial intrusions into their respective environments via content management system (CMS) vulnerabilities on their respective websites [21, 22]. In both cases, limited information indicates CMS vulnerabilities were leveraged by Berserk to upload malicious variants of the companies' software packages.

All three of the impacted companies are (or were, in the case of *MESA*) based in European countries. Furthermore, analysis of product applications and use indicate the respective software items were largely focused on or only present in European

markets. Even more interesting, in the case of *MB ConnectLine's mbCHECK*, which had both North American and European software versions, only the European version was modified even though the CMS vulnerability used would have allowed for both products to be replaced with malicious variants. Although other manufacturers may have been impacted in this event, the above observations strongly suggest a primary targeting focus on Western European industrial entities for this portion of Berserk operations.

Technical examination of the modified binaries shows a common artifact in the Portable Executable (PE) header of each: an '.ndata' section with a raw size of zero but a large virtual size, indicative of packed or compressed software. In this case, the observations align with a specific packaging mechanism: the Nullsoft Scriptable Install System (NSIS). Although designed for legitimate use, various malicious entities utilize NSIS packaging to obfuscate malware or evade detection.

Nearly all the original, unmodified binaries do *not* use NSIS for packaging software. Looking at PE header information between the malicious items associated with Berserk activity and pre- and post-attack software, the legitimate software items feature dramatically different structures from the NSIS-packaged Berserk items.

```
#####
[0] File: legit/mbCHECK.exe
#####
Meta-data
=====
Size           : 1681032 bytes
Type           : PE32 executable (GUI) Intel 80386, for MS Windows
Architecture   : 32 Bits binary
MDS            : 16a549c9e0d79046671660ffdc87fe4e
SHA1           : 76b63e6b9032ee0a19396e2e76115c6e0ccc3137
SHA256        : 81218543789aaf17e01cb104c099afd38279ee801365526a377e4b29a359022
Date          : 0x53A961A1 [Tue Jun 24 11:31:45 2014 UTC]
CRC: (Claimed) : 0x1a5df9, (Actual): 0x1a5df9
Language      : LANG GERMAN, SUBLANG GERMAN
Entry Point   : 0x5401a4 .itext 1/9 [SUSPICIOUS]

Sections
=====
Name           VirtAddr      VirtSize      RawSize      MD5                               Entropy
-----
.text          0x1000        0x13d58c     0x13d600     efc6e15686a5a16584e0ed578e427ca1 6.374249
.itext         0x13f000      0x1210       0x1400       5e3e9e9033248a4969693260483be0ed 5.780299
.data          0x141000      0x9218       0x9400       37ff1439c83bd961f25e846174e4872a 5.716039
.bss           0x14b000      0x5b08       0x0          d41d8cd98f00b204e9800998ecf8427e 0.000000 [SUSPICIOUS]
.ndata         0x151000      0x3206       0x3400       628ca9d47c9f1906a8b17cf15b73cd7 5.106632
.tls           0x155000      0x3c         0x0          d41d8cd98f00b204e9800998ecf8427e 0.000000 [SUSPICIOUS]
.rdata         0x156000      0x18         0x200       05782a81d1dc4d65d450abe2f1cb2db4 0.210826 [SUSPICIOUS]
.reloc         0x157000      0x14344      0x14400     107e47ab2750ebdb01b9e0f86e237344 6.644911
.rsrc          0x16c000      0x39200      0x39200     86838bbd5deb7f627e7ea39c8dcde691 6.332215

#####
[0] File: 0b74282d9c03affb25bbecf28d5155c582e246f0ce21be27b75504f1779707f5
#####
Meta-data
=====
Size           : 1141478 bytes
Type           : PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Architecture   : 32 Bits binary
MDS            : 1d6b11f85debdda27e873662e721289e
SHA1           : 7f249736efc0c31c44e96fb72c1efcc028857ac7
SHA256        : 0b74282d9c03affb25bbecf28d5155c582e246f0ce21be27b75504f1779707f5
Date          : 0x51E3058F [Sun Jul 14 20:09:51 2013 UTC]
CRC: (Claimed) : 0x0, (Actual): 0x11eace [SUSPICIOUS]
Language      : LANG ENGLISH, SUBLANG ENGLISH US
Entry Point   : 0x40310b .text 0/5 [SUSPICIOUS]

Sections
=====
Name           VirtAddr      VirtSize      RawSize      MD5                               Entropy
-----
.text          0x1000        0x5de8       0x5e00       fale76d307e7273bee64c0b28254b0d6 6.503326
.rdata         0x7000        0x12da       0x1400       4a7a1dd8d6a3e41ec67f817a3ebd35ce 5.095967
.data          0x9000        0x25c98      0x400       d06b65bfc666e46c98b261b105bdc5bd 5.037908
.ndata         0x2f000       0x8000       0x0          d41d8cd98f00b204e9800998ecf8427e 0.000000 [SUSPICIOUS]
.rsrc          0x37000       0x18058      0x18200     886332df04c86a57666c23593d3f9935 7.565335 [SUSPICIOUS]
```

Figure 3: Comparison of PE headers for *mbCHECK* installer.

Although definitive evidence does not exist, what information is available strongly suggests that Berserk modified the original binaries to package them, along with other components, with NSIS. This technique is not unique to Berserk and is reflected in activity ranging from ransomware to targeted intrusions.

Of note, the *MESA Imaging SwissRanger* software *legitimately* used NSIS packaging in benign versions of the software before and after the Berserk-related events. In this case, it is unclear precisely how Berserk modified the binary, unless access to source packages and related items allowed the entity to repackage the NSIS installer to include malicious functionality.

In all observed cases, the modified ICS-related binaries typically contain similar functionality: deploying an encoded Havex DLL payload to victim machines. Specific deployment characteristics and filesystem location change depending on the variant. But in all publicly known cases, modified installers drop the Havex DLL to disk then launch it via 'rundll32' calling a 'RunDllEntry' export, passing execution on to the malware.

Havex malware

All available information and third-party reporting indicate that the ultimate purpose of original Berserk activity (the 'Dragonfly campaign') was delivery and installation of Havex malware. While delivered in various ways, including in some

cases through intermediate malware (described briefly below), Havex represents the identified, known end-goal of these early 2010s intrusions.

Havex serves as scaffolding around which other capabilities can be built, working in a modular fashion to incorporate additional functionality given Berserk's intentions or purpose. As such, Havex on its own is a mere loader for other capabilities. Berserk delivered Havex as a DLL, typically embedded in other objects, which injects further code into the *Explorer* process. Once running in the context of a trusted program, Havex reaches out via its command-and-control (C2) communications to check in with its operators, and download additional functionality or modules [6, 23]. Havex persistence is relatively simple, writing itself to disk (usually *%AppData%*, *%TEMP%* or *%System32%*) and creating an auto-start registry key.

Havex only begins to become interesting when examining the follow-on modules that provide functionality. Based on reporting from multiple security vendors, Berserk used compromised, legitimate websites to host C2 and Havex modules, a trend which would continue through subsequent Berserk activity post-Dragonfly. Module functionality includes several typical intrusion capabilities: system profiling, network enumeration, password theft, and similar post-exploitation activities.

However, Havex also included specialized modules with a then-unique purpose: enumerating and mapping ICS-specific systems in victim environments. Although relatively primitive, examination of the various modules shows a definite emphasis on ICS-related processes and protocols [24, 25]. For example, a network scanner module used in Havex operations features relatively straightforward scanning functionality, but does so with a particular interest in hard-coded ICS-related ports, as described in Table 2.

Port number	Associated service or software
102	Siemens SIMATIC PLC Communications
502	Modbus over Ethernet
11234	Measuresoft ScadaPro Communications
12401	7-Technologies Graphical SCADA, GE Proficy License Server Manager, WllinTech KingSCADA
44818	Rockwell Automation ControlLogix and RSLinx, Tec4Data SmartCooler, Cisco IOS Common Industrial Protocol processor

Table 2: Hard-coded ICS-related ports.

For emphasis: the above are the *only* ports scanned on the /24 subnet of the executing machine. Other, typical ports enumerated such as remote access services are simply not present. Such behaviour indicates specific intentions to identify a relatively narrow range of industrial products.

In addition to the above module, Havex also incorporates a protocol-specific enumeration utility focusing on the Open Platform Communication (OPC) standard [6, 24, 26, 27]. The module enumerates OPC servers to identify clients and related information, but no known functionality exists to deliberately interact with or modify OPC functionality. As written, all publicly identified examples of this module appear to be reconnaissance-focused, with no capability to intentionally cause disruption or manipulation of industrial systems.

Although not designed to cause disruption, testing of Havex's OPC module reveals some concerning features. When tested in certain environments, the OPC module induces OPC server crashes, which have the possibility of inducing follow-on process instability [28, 29]. Uncontrolled process termination in industrial environments can lead to a number of consequences, from short-term loss of visibility to potential process destruction. That the OPC enumeration feature contained this ability is indicative of either a lack of thorough testing by Berserk-supporting developers, or a callousness with respect to potential consequences from running such a tool. The implications of this will be examined shortly.

Other observed malware tools

In addition to Havex, the Dragonfly campaign is associated with several other tools. Although in several cases not exclusive to the actor, the other items were also present in early Berserk activity:

- Karagany, a remote access and information-stealing tool used as an intermediate item prior to the deployment of Havex [5, 30]. The malware is based on leaked code from the earlier crimeware-focused DreamLoader framework [31], and as such cannot be considered exclusive to Berserk operations.
- Sysmain, a remote access tool packaged as a DLL for information gathering and follow-on command execution [6]. While otherwise unremarkable, analysis from *Kaspersky* indicated that in at least some instances, compromised *MESA Imaging* software delivered Sysmain as its payload rather than Havex, making it an exception to the majority of observed supply chain compromises. This feature is also significant as *MESA Imaging* products were originally packaged via NSIS, unlike other vectors which were modified to do so.

- DDex, a lightweight downloader with persistence capability [6]. The malware takes its name from observed instances in the wild, named 'ddex.exe'. Of note, in the few samples available for analysis, file names and paths are hard coded, indicating a somewhat brittle tool used as an intermediary to load additional functionality.
- ClientX, which, based on analysis from *Kaspersky*, is functionally identical to Sysmain, but written in .NET [6].

Other than Karagany, the remaining tools associated with early Berserk operations are only documented in reporting from *Kaspersky* relating to what it refers to as 'Crouching Yeti'. Yet other than Karagany's origins in leaked code, the remaining tools all appear to be uniquely associated with early Berserk operations with no evidence of widespread use. The latter point is further emphasized in that, while the Dragonfly campaign featured analysis from multiple organizations, only one entity (*Kaspersky*) identified (or at least publicly documented) payloads beyond Havex and Karagany in reporting.

Campaign targeting

The Dragonfly campaign started no later than 2010 and appears to have concluded in 2014 following public disclosure. During this period, the threat actor impacted several entities. Yet the precise geography and industry vertical of victims shifts depending on what public reporting one consults. For example, reporting from *Symantec* and *CrowdStrike* emphasize energy sector entities across Europe and North America as primary victims in the Dragonfly campaign [5, 7]. However, reporting from *Kaspersky* shows quite widespread activity, including multiple victims in South America, Central and Southeast Asia, and the Russian Federation, with significant representation from educational and government entities among known victims [6].

Based on the above, the Dragonfly campaign appears confusing. Depending on the source, the campaign either appears focused on ICS-related entities and critical infrastructure, or functions as a much wider targeting entity among both critical infrastructure and traditional espionage targets. From a broader cyber threat intelligence (CTI) perspective, this situation highlights how different types of visibility into events can produce different conclusions.

In the case of early Berserk behaviours, the Dragonfly campaign appears to be widespread in overall nature. However, by 2013, the combination of SWC targets, specific Havex modules, and documented victimology strongly suggests the main thrust of the later stages of the Dragonfly campaign was gaining initial access to and performing reconnaissance of industrial and critical infrastructure entities. Such activity took place across the oil and gas and manufacturing verticals in Europe and North America, with potential for activity in other regions as well. While concerning, such intrusions appear to have stopped at information gathering without any disruptive impact or clear intention to deliver such an effect, or so it would seem.

POSSIBLE DESTRUCTIVE INCIDENT

While there is nothing publicly known about the Dragonfly campaign and early Berserk activity, or in the capabilities of any software associated with these activities, that indicates such actions were intended to disrupt critical infrastructure environments, this observation does not remove the possibility of *unintentional or accidental* disruption while operating in such networks. Given the environments in which Berserk operated during parts of the Dragonfly campaign, even though the group *likely* did not have disruptive intent, the possibility exists for unintended consequences in sensitive environments.

Reviewing Havex functionality, interesting possibilities emerge. When looking specifically at the OPC enumeration utility, testing in multiple environments demonstrated that this utility could cause a scanned OPC server to crash. Depending on error handling and other controls, such an abrupt event could result in follow-on process instability. Therefore, while the Dragonfly campaign appears to focus on espionage or, at worst, initial access to sensitive environments for later operational flexibility, the mere execution of one of the responsible entity's survey programs could result in inadvertent disruption.

In an annual review of events taking place in 2014, the German Bundesamt für Sicherheit in der Informationstechnik (BSI) disclosed a disruptive incident at an unnamed steel mill resulting in physical destruction [32, 33]. Unfortunately, many specific details around this event, including precisely when it occurred, were not provided in BSI's reporting. Yet given when the report was released, as part of a review of events in 2014, we can assess with moderate confidence that the event took place in 2014, and with high confidence (given the volatile nature of digital evidence to assess this as a cyber incident) that the event took place not long before then. This tentative timeline would place the steel mill incident in the same period of time as the Dragonfly campaign.

Reviewing limited details of the steel mill event, BSI reporting indicates that unnamed intruders leveraged spear phishing to gain credentials from users in the victim environment to enable initial access. The intruder then pivoted throughout the environment until actions resulted in multiple components of the victim entity's blast furnace to fail, inducing physical damage.

Although none of the reporting or analysing entities at the time of the incident made conclusive attribution statements, with the benefit of hindsight we can draw some potential conclusions. While the tradecraft (loosely) documented in BSI reporting (phishing and credential capture for lateral movement) is rather common, such activity also aligns with Berserk operations in the Dragonfly campaign, and closely aligns with follow-on Berserk actions documented below. Additionally, the Dragonfly campaign featured extensive intrusions into European manufacturing organizations from at least 2010 through 2014, which links to the steel mill incident in terms of industry vertical and geography. Finally, the unstable nature

of the OPC enumeration payload of Havex could induce process instability through ICS disruption, which could yield a potentially destructive result, depending on the environment.

While insufficient evidence exists in publicly available resources to confirm any of the above observations, the combination of timing, victimology, and (inadvertent) capability points to Berserk Bear as a likely suspect for inducing the steel mill incident. Even though the event was almost certainly unintended, the effects produced show the risks inherent in operating in critical infrastructure or similar environments.

RESURGENCE: DRAGONFLY 2.0 TO PALMETTO FUSION

Following multiple public disclosures in 2014, Berserk-related activity appeared to cease after the Dragonfly campaign. Yet in 2017, researchers at *Symantec* disclosed a new campaign of phishing (combined with SWC) designed to capture credentials from victims [34]. This reporting was reflected in subsequent US government notifications [35], which were later revised to indicate a link to Russian state-sponsored activity [36]. Although the *Symantec* and US government reporting overlap, analysis of specific behaviours, targeting and tooling indicates a bifurcation in campaigns. *Symantec*'s Dragonfly 2.0 activity appears aligned with targeting of Turkey and European entities from late 2015 through 2017, while US reporting, referenced as 'Palmetto Fusion' in initial disclosures, targeted US and UK electric sector entities from 2017 through at least 2019 [37, 38].

Given disclosures in 2014, Berserk appears to have taken only a short break in operations between the original Dragonfly campaign and this activity. Within that time though, the group substantially modified operations while preserving enough technical and other links to associate this activity with previous campaigns. While behavioural characteristics of the activities shifted, which would justify tracking this activity (including components of these campaigns) as separate behavioural clusters, sufficient evidence exists combined with government disclosures to justify linking all these activities back to the same likely 'sponsor' or entity under Berserk Bear.

Continued phishing and strategic website compromise

As with the Dragonfly campaign, Dragonfly 2.0 and Palmetto Fusion leveraged phishing and SWC for initial access purposes. However, while targeting characteristics (focus on energy-themed entities and concepts) were similar to earlier activities, actual functionality was substantially different. Rather than utilize malicious documents or SWC to directly deploy capabilities (e.g. exploits or malware) on victim systems, all observed items in this campaign instead used functionality in *Windows* operating systems to generate an outbound Server Message Block (SMB) communication to adversary-controlled infrastructure. If successful and collected, Berserk would then harvest NTLM credentials from this connection to replay for remote access into victim environments, potentially via tools such as Responder [39].

Fun with Phishery

Public indications of energy sector-focused phishing activity first appeared in July 2017 from researchers at *Cisco Talos* [40], although parallel non-public reporting existed in US government circles followed by media disclosure of some high-profile victims [41]. Malicious documents leveraged implementations of an open-source tool called Phishery for injecting a remote resource, prompting an outbound SMB connection, into the file [42].

While technically rather simple, targeting and document construction appears to be quite specific to victim organizations and industry verticals. For example, initial phishing activity linked to Dragonfly 2.0 targeted a Turkish oil and gas entity using a holiday party theme, and an unnamed entity spoofing ISO 27001 awareness.



Figure 4: Phishing samples, Dragonfly 2.0.

Later examples, more closely aligned with the Palmetto Fusion activity documented by the US government, generally used well-crafted resumes for power engineers as lures with an ultimate focus on US and UK targets in the electric sector.

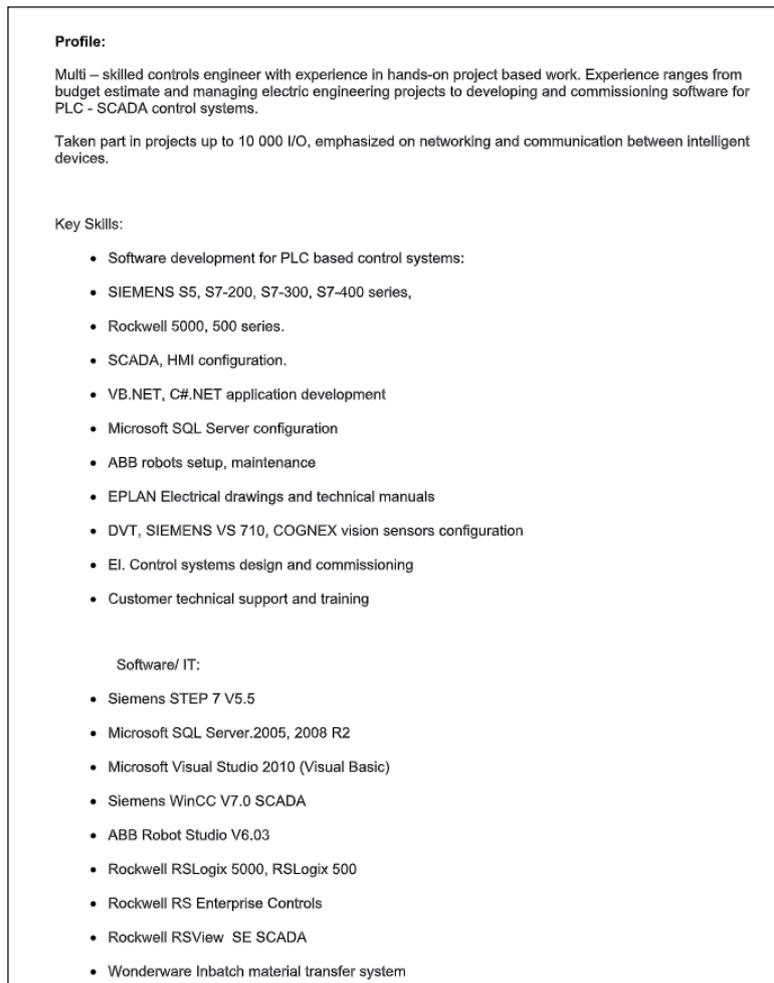


Figure 5: Palmetto Fusion resume phish.

Although straightforward, the phishing campaigns in question, especially the later Palmetto Fusion stages, are interesting given strategic targeting of service providers as intermediate victims. As documented by Rebecca Smith and Robert Barry, the entities responsible for this campaign appeared to compromise various contractors and other entities first, and used these entities to then distribute the malicious emails and credential leaking documents to electric utility victims [43]. In this fashion, trust-subversion tactics previously observed in the Dragonfly campaign resurfaced, but this time targeting service relationships rather than software dependencies. Through a sequence of intermediate compromises, Berserk could move from service providers to ultimate victims, leveraging existing trust relationships to improve the likelihood of successful interaction with malicious attachments.



Figure 6: Palmetto Fusion campaign targeting sequence.

Leaking credentials from websites

SWC activity related to Dragonfly 2.0 and Palmetto Fusion activity followed the same behavioural pattern as the malicious documents: leaking credentials from victims, and not delivering exploits or malicious payloads directly. While avoiding such active content in modified web pages, these campaigns continued an emphasis on energy and related entities, as seen in the list of compromised sites involved in the incident (Table 3).

Website	Campaign	Description
ameresco[.]com	Dragonfly 2.0	US-based renewable energy-focused engineering services.
cfemedia[.]com	Dragonfly 2.0	US-based online publisher.
cfemedia.gcnpublishing[.]com	Dragonfly 2.0	US-based online publisher.
controleng[.]com	Palmetto Fusion	Control system engineering publication.
csemag[.]com	Palmetto Fusion	Engineering-focused publication
gama[.]com.tr	Dragonfly 2.0	TR-based holding company including energy investments.
grand-central[.]net	Dragonfly 2.0	Customer data platform.
oilandgaseng[.]com	Palmetto Fusion	Oil and gas engineering publication.
plantengineering[.]com	Palmetto Fusion	Control systems engineering publication.
reenergyholding[.]com	Dragonfly 2.0	Renewable energy company.
turcas[.]com.tr	Dragonfly 2.0	TR-based oil and gas company.

Table 3: List of compromised sites involved in the incident.

Implementation of SWC varied depending on timing and targeting. Dragonfly 2.0 targeting of European and Turkish energy entities used a nested mechanism for redirecting queries, potentially acting as a filtering mechanism and similar to earlier Dragonfly activity, before arriving at the ultimate resource inducing the SMB connection [44]. A modified PHP object first directs to one Virtual Private Server (VPS) via HTTP, which then attempts to retrieve a file object via SMB from a different VPS instance.

Later activity, corresponding with the largely US- and UK-focused Palmetto Fusion activity, appears to focus on compromise of the TYPO3 Content Management System (CMS) to modify a JavaScript object (typically jquery.easing.js). CMS targeting, while not uncommon, links to the subversion of ICS software providers in the Dragonfly campaign. During Palmetto Fusion operations, multiple websites for power, energy, and engineering publications featured a modification to the same resource with the following path:

/typo3conf/ext/t3s_jslidernews/res/js/jquery.easing.js

When loaded, the modified library attempts to retrieve a 1x1 pixel image referencing an external object to prompt the external authentication attempt. Unlike the Turkish campaigns taking place earlier, this activity directly references adversary-controlled infrastructure as opposed to using redirects to obfuscate activity or introduce possible filtering.

```

    });
    var i = document.createElement("img");
    i.src = "file:///184.154.150.66/ce.png";
    i.width = 1;
    i.height=1;
    document.getElementsByTagName("body")[0].appendChild(i);
    /*

```

Figure 7: Injected code example.

In addition to distinctions in direct reference of external resources, the two campaigns also feature differences in infrastructure characteristics. While the Dragonfly 2.0 campaign appears to largely rely on adversary-owned and -controlled VPS infrastructure, the Palmetto Fusion campaign almost exclusively leverages legitimate, compromised network infrastructure. As documented by *Kaspersky*, parallel Berserk-related operations focused on gathering infrastructure through server compromise, both to deploy SWC and to provide infrastructure to receive leaked credentials [45].

Change in tools and deployed capabilities

Although the Dragonfly 2.0 and Palmetto Fusion campaigns represent near continuous operations from late 2015 through at least 2019, substantial differences in post-intrusion behaviour align with the geographic and temporal separation in campaigns. Differences are significant enough that, using behaviour-focused attribution methodologies, the campaigns could be taken as the actions of separate, distinct activity groups. Yet identified overlaps in infrastructure, targeting and some techniques indicate that, at minimum, these operations were executed by entities pursuing similar objectives, if not separate teams within the same organization.

Earlier activities corresponding to Turkish and other targeting in the Dragonfly 2.0 campaign closely resemble the original Dragonfly activity in many characteristics. While initial access mechanisms are noticeably different, post-intrusion tradecraft mirrors original Dragonfly operations through the use of a combination of various types of malware, including some types narrowly associated with Berserk operations such as Karagany variants and a unique backdoor referred to by *Symantec* as Heriplor, closely linked to Havex-related payloads from the Dragonfly campaign [34].

Later activity, aligned with the Palmetto Fusion phase of operations, shifted behaviours noticeably. While Berserk employed similar intrusion techniques to the Dragonfly 2.0 activity (credential-leaking phishing and SWC), post-intrusion behaviours were substantially different. Particularly, these operations featured the near-complete absence of any custom tooling or malware. Instead, lateral movement and post-exploitation activity focused on a combination of continuous credential capture and reuse and the deployment of either legitimate tools used maliciously or publicly available frameworks for intrusion operations, such as the PSEXec utility or leveraging system commands to create and enable adversary-controlled accounts.

ICS-specific activity

In the Palmetto Fusion phase of operations, reporting from multiple commercial, media and government entities confirms that Berserk sought and, in several cases, succeeded in gaining access to industrial environments, including control systems. Yet unlike the Dragonfly campaign, no ICS-specific tooling or capability, such as Havex's OPC item or related port scanners, were identified. At first glance, this appears to represent a devolution of capability, moving from ICS-aware software to only using native commands and similar for reconnaissance purposes.

Yet given the previous discussion of the German steel mill incident and its potential connection to the Dragonfly campaign, this operational change may represent an adjustment following that event. If Berserk was responsible for this incident, after (inadvertently) causing a disruptive incident through the somewhat buggy OPC polling entity, Berserk appears to have modified its tradecraft to avoid capabilities that would result in similar unintended consequences. Particularly given that this campaign largely focused on critical infrastructure entities in the US, an accidental disruption in these environments would presumably be quite costly or risky, arguing for greater caution.

Berserk's restraint is shown in what actions the entity took in control system environments: searching for and copying items such as remote access profiles and control system-related documentation. When accessing more sensitive equipment, such as human-machine interfaces (HMIs) within a victim environment, Berserk deployed a custom tool to take a screenshot of the system which was exfiltrated via existing remote access mechanisms, shown in Figure 8.

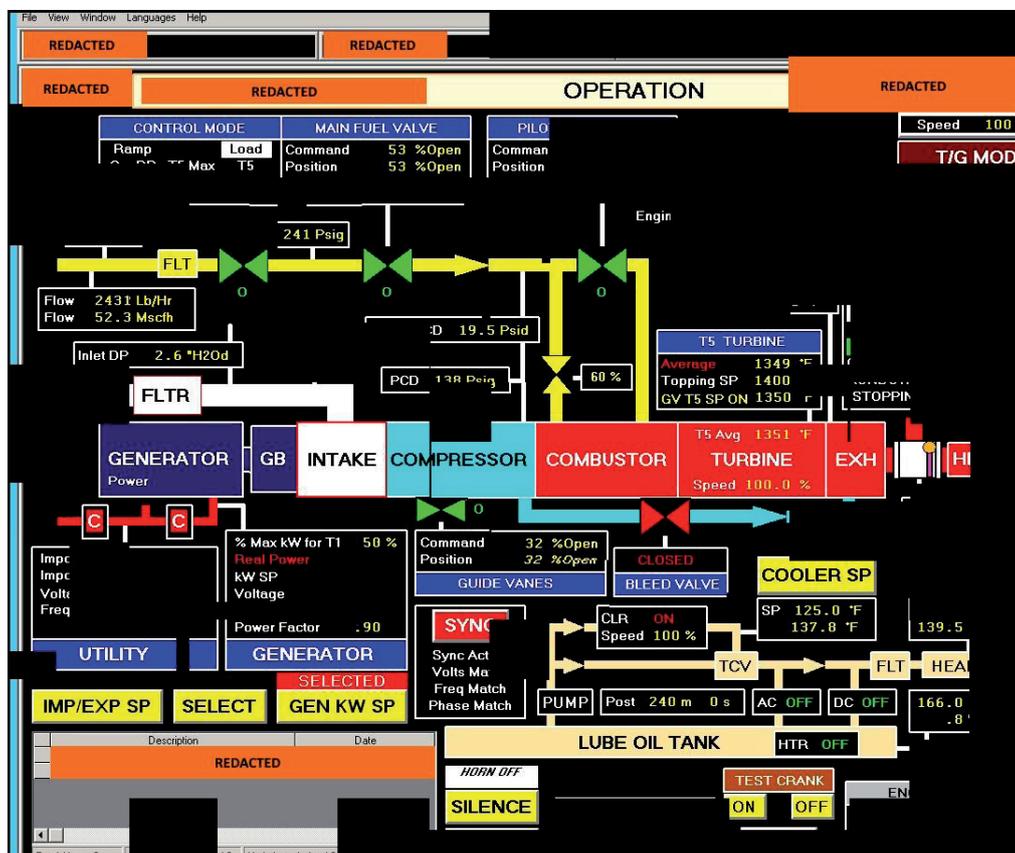


Figure 8: Exfiltrated screenshot of victim HMI.

Thus, while Berserk’s ability to access these environments is quite concerning, all available evidence indicates this entity sought to avoid any potential disruptive or unintentionally destructive impact. Whether this is a result of learning from the steel mill incident, or an abundance of caution given the targets, we can look at these ICS-related intrusions as representing access development and information gathering (potentially to enable future operations) as opposed to an immediate ‘attack’ or similar [46].

Distinguishing Dragonfly 2.0 and Palmetto Fusion from Dragonfly

Reviewing activity from Dragonfly to Dragonfly 2.0 to Palmetto Fusion, we can observe a steady evolution in operations and behaviours through each campaign. Illustrated Figure 9, we observe overlaps from one campaign to the next, but sufficient development such that Dragonfly and Palmetto Fusion ultimately look like separate operations aside from overlaps in targeting. Without the Dragonfly 2.0 activity serving as a vital link between the two, with its continued use of Dragonfly-related tools but introduction of credential harvesting as a primary mechanism which the Palmetto Fusion phase would rely on almost exclusively, drawing a line of continuity through these activities would be problematic. Yet because of this iterative nature between campaigns, with only some aspects altered while others remain the same, we can link these groups together as likely phases for the same entity, Berserk Bear.

Berserk Bear-Linked Campaigns				
	Dragonfly	Dragonfly2.0	Palmetto Fusion	Recent Activity
Timing	2010(?) - 2014	2015-2017	2017-2019(?)	2018(?)–Present
Target Geography	Europe, North America	Turkey, Europe, North America	United States, United Kingdom	United States, Ukraine, Germany
Target Sectors	Manufacturing, Oil & Gas, Electric, Education	Oil & Gas, Electric	Electric	Electric, Oil & Gas, Transportation, Elections, Media
Infection Vector	Phishing, SWC, Supply Chain	Phishing, SWC	Phishing, SWC	Traffic Shaping, SWC
Persistence Mechanisms	Registry Keys, LNK Files	Registry Keys, LNK Files	LNK Files, Credential Harvesting	Credential Harvesting
Impacts or Effects	Possible Destructive Event	Data Collection, Access Development	Critical Infrastructure Control System Access	Unknown

Figure 9: Comparing Dragonfly, Palmetto Fusion and Dragonfly 2.0.

NETWORK INFRASTRUCTURE INTRUSIONS

Concurrent with Palmetto Fusion activity in 2018, US and UK government reporting identified another campaign targeting critical infrastructure environments [47, 48]. Subsequent discussions with victims and other sources indicate that the electric sector was a primary, although not exclusive, target of this campaign. While US and UK sources did not attribute this campaign to any specific threat actor (other than identifying it as Russian in origin), several items tangentially link this activity to Berserk:

- Targeting of critical infrastructure sectors directly and indirectly through service provider relationships (in this case, Internet service providers).
- Timing that overlaps with the Palmetto Fusion phishing and SWC campaign.
- Use of credential harvesting and replay to enable access and subsequent operations in victim environments.
- Leveraging built-in system functionality and tools to modify configurations and other items for malicious purposes.

While the above indicate a potential link, operations against network infrastructure devices such as routers would represent a significant departure from known Berserk behaviours going back to the Dragonfly campaign. The identified activity may represent a link to the same ultimate decision-making authority within Russian intelligence operations, but behaviourally appears too distinct to firmly link to Berserk based on publicly available information.

Recent activity

Beginning in 2019, SWC activity resembling previous Berserk operations in the Dragonfly 2.0 and Palmetto Fusion campaigns reappeared. While remaining largely focused on critical infrastructure entities, targeting scope expanded to include entities such as airports, government and election authorities, and general media items.

Ukrainian political and energy entities

In early to mid-February 2019, various websites in Ukraine featured compromises similar to past Berserk operations. In addition to targeting the Ukrainian energy sector, such as injecting into various subdomains for Ukrainian energy conglomerate Dtek, the campaign expanded in May 2019 to include various media and cultural entities.

Website	Description
dtek[.]com	Ukrainian energy conglomerate.
unn[.]com[.]ua	Ukrainian media entity.
ntn[.]ua	Ukrainian media entity.
zomua[.]tv	Ukrainian media entity.
fcdynamo[.]kiev[.]ua	Ukrainian football club.

Table 4: Ukrainian websites featuring compromises.

In many cases, these compromises persisted through at least late 2020 [49]. Examination of specific SWC instances shows a combination of injecting into static web pages, a tactic not observed in earlier activity, and modifying various JavaScript items in a manner nearly identical to the Dragonfly 2.0 and Palmetto Fusion campaigns.

From a targeting perspective this activity shows flexibility in what appear to be Berserk-related operations. In terms of timing, initial compromises coincided with Ukraine's 2019 presidential election. From this, we can hypothesize that Berserk-related operations were 'retasked' to cover this strategically significant event (from a Russian perspective). While this seems plausible, the very broad nature of some of the targets, including major general media sites and a popular football club, indicates a very wide, unfocused net for activity. This lack of specificity is further emphasized by the lack of intermediate, 'screening' links as seen in historical Berserk-related activity.

Airports and Western infrastructure

In April 2019, multiple entities identified a modification to San Francisco International Airport's website (the primary web page, and a mirrored resource) [50]. Further analysis revealed a SWC incident essentially identical to historical Berserk activity. Additional research identified over a dozen other airports in the United States exhibiting similar signs of compromise in 2020, indicating a potential expansion of Berserk-related activity to transportation-related entities. Of note, available evidence does not appear to indicate targeting of the airports as the primary objective, but rather inducing the same credential leak behaviours to target visitors to the airport websites.

Subsequent reporting in October 2020 identified further intrusions into transportation and local government networks in the US [51, 52]. Most worrying about these intrusions, events appeared to extend into election and related infrastructure in line with the 2020 US Presidential election. In this sense, activity mirrors the earlier Ukraine-focused activity, in being linked to a major political event. As with other Berserk activity, the event is not linked to any known, attempted disruptive activity, and likely represents either intelligence gathering or, at most, opportunistic prepositioning for future operations. Nonetheless, this extension to election-related infrastructure in state and local government networks represents a worrying expansion in targeting.

RELATIONSHIP TO RUSSIAN-LINKED CYBER OPERATIONS

Although the original Dragonfly campaign largely evaded any specific attribution, the US and UK governments subsequently linked Dragonfly 2.0 and Palmetto Fusion campaign activity to Russian intelligence operations [36, 53]. While such statements establish a degree of high-level responsibility for events, such 'general attribution' claims are not especially helpful for network defenders and critical infrastructure operators [54].

Russian-nexus cyber operations targeting external entities largely break down into actions guided or executed by teams under three entities: the Military General Staff's Main Intelligence Directorate (GRU), the Federal Security Service (FSB), and the Foreign Intelligence Service (SVR) [55]. In addition to academic interest in aligning cyber operations with their likely sponsor organization, the missions and behaviours of these different organizations can give us insight into potential intentions and purpose. For example, GRU-aligned entities possess a history of engaging in direct, deliberate disruptive operations, such as the Ukraine power events and similar incidents tied to the GRU's Main Center for Special Technologies, Unit 74455, commonly referred to as Sandworm [4, 56]. Meanwhile operations associated with the SVR, although at times

involving critical infrastructure sectors, are exclusively linked with intelligence gathering and similar activity, even in recent widespread campaigns such as NOBELIUM-related activity. [57] [58]

Given Berserk's continued operations against critical infrastructure targets for over a decade, understanding how this group aligns with more general Russian-nexus cyber operations can be quite valuable in determining potential motivations. For example, alignment with GRU entities would indicate the potential for rapid movement from intrusion to deliberate disruptive or destructive actions, while alignment with either of the civilian intelligence agencies (FSB or SVR) would strongly suggest either an intelligence or long-term 'prepositioning' focus rather than attempting immediate impacts.

In 2018, the UK's NCSC published a lengthy list of disruptive or controversial operations linked with various elements of the GRU [56]. The list includes high-profile incidents such as the Ukraine electric sector attacks along with other operations, but notably omits elements of the Palmetto Fusion campaign (which also targeted the UK electric sector) and the network infrastructure compromises discussed previously that may also link to Berserk operations [48]. Although unfortunately not definitive, the lack of any public link between Berserk operations with GRU-related incidents allows us to provisionally conclude that Berserk is not part of Russia's military intelligence apparatus, with its history of launching disruptive events.

If we begin to look at Russia's civilian intelligence organizations, the SVR and FSB, other possibilities begin to emerge [59]. Although no threat actor associated with the SVR or FSB is associated with a high-profile critical infrastructure event such as the Ukraine attacks, and responsibility for the 2017 Triton event remains unknown beyond general Russian responsibility [60, 61], various campaigns linked to these entities have previously touched industrial and critical networks. Examples include the NOBELIUM campaign, along with historical activity linked to SVR-associated APT29 [62, 63].

The above observations are supported by limited information, primarily leaked from government sources, indicating that Berserk likely resides under FSB authorities [37, 41]. Reviewing available evidence, this appears to make sense for several reasons:

- Lack of known, intentional disruptive operations against critical infrastructure (assuming Berserk is responsible for the steel mill incident, and that this was an accident).
- Absence of any group consistently targeting critical and industrial infrastructure linked to FSB authorities among Russian intelligence agencies.

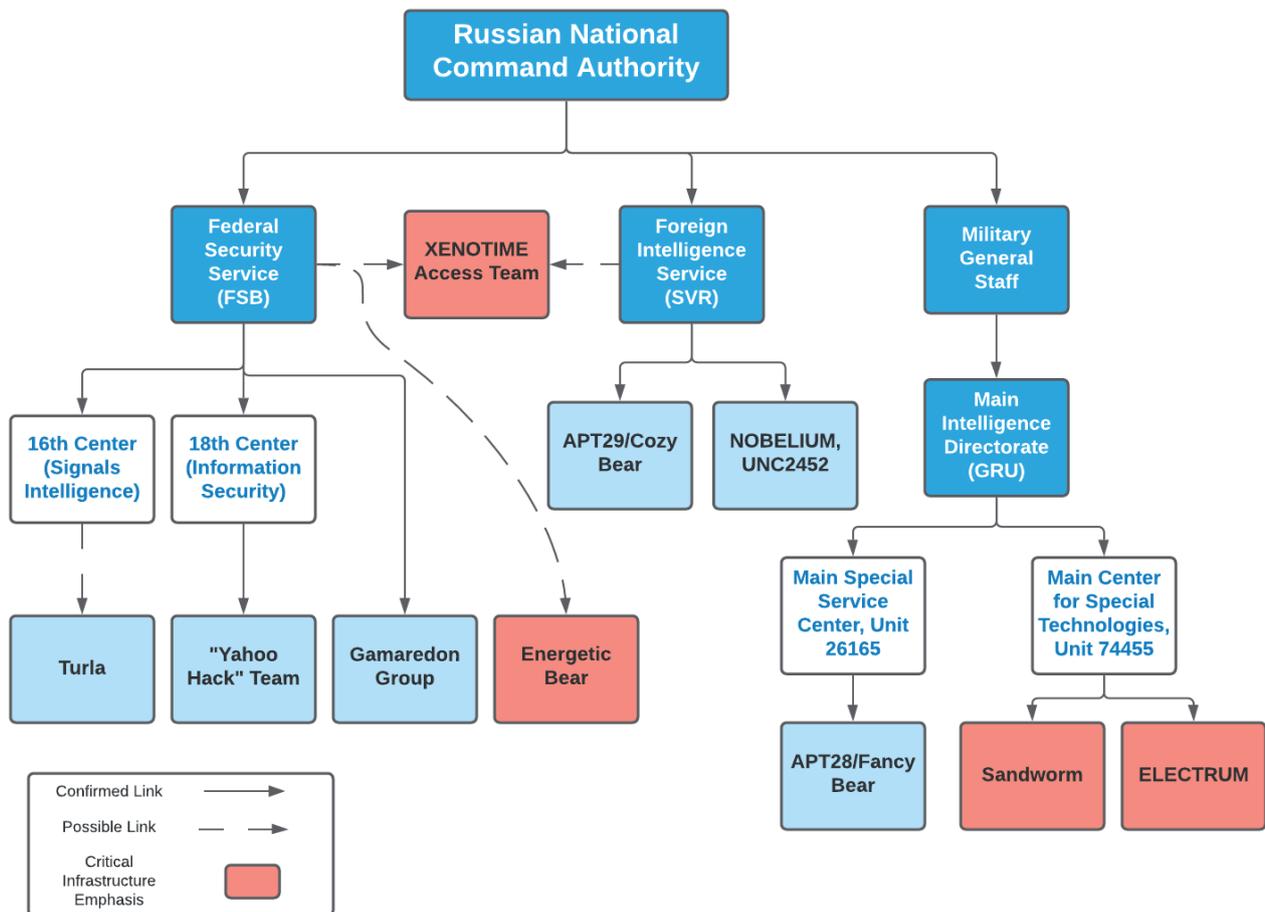


Figure 10: Overview of Russia-linked cyber actors.

- Possessing independent, unrelated ICS-related capabilities from all other entities linked to Russian intelligence operations.

Unfortunately, most of the above items are simply stating what Berserk is *not* (specifically, not the GRU, and probably not the SVR) rather than saying what Berserk actually *is*. As such, while multiple sources imply a link between Berserk Bear and Russia's FSB, publicly available evidence does not exist at this point to solidify this link. Yet even though we have failed in deriving specific attribution for Berserk, we can still make reasonable claims with respect to Berserk's operations and likely intentions: to gather intelligence on and access to targets of interest, but likely not to move toward immediately using such access for disruptive purposes except in extreme circumstances (such as armed conflict).

CONCLUSIONS

Berserk Bear, an entity known by many names over many years, carved a fascinating history through operations targeting multiple facets of European and North American critical infrastructure entities. Aside from the group's longevity (taking behavioural evolutions into account), the group also demonstrated the capability to interact with ICS-related environments through multiple mechanisms. Yet despite the group's history and technical prowess, it frequently receives second billing (at best) relative to other Russian-linked entities such as Turla, Sandworm and NOBELIUM.

Berserk may be overlooked because in many respects (aside from the potential steel mill incident) it represents the 'dog that didn't bark'. For all the group's activity, it is not linked to any single, definitive incident or disruptive event that would garner headlines and attention. While operations from the Palmetto Fusion campaign through the present indicate expanding appetites for the group, there is no Triton incident or large-scale power disruption associated with the entity.

But adopting this view is myopic to say the least, and quite likely dangerous given Berserk's demonstrated capabilities. Principally, Berserk Bear has repeatedly demonstrated the willingness and ability to penetrate industrial and critical infrastructure environments for over ten years. In doing so, the group has almost certainly facilitated significant intelligence gathering, capability development, and potentially effects pre-positioning in highly sensitive networks. While available information indicates Berserk has not deliberately engaged in disruptive acts thus far, the group has laid the groundwork for potentially crippling attacks through its persistence and ability to generally avoid significant attention. While a Berserk Bear intrusion may not be associated with an immediate attack like some other Russian-linked intrusion sets, asset owners and network defenders would do well to treat any sign of this group as deeply worrisome. While Berserk's impacts may be delayed, the group remains one of the most stubborn and capable entities willing to dive straight to the heart of vital networks across multiple industry verticals and geographies.

ACKNOWLEDGEMENTS

The above analysis and research spans multiple organizations and individuals. In addition to *Gigamon*, who enabled the completion of this work, the author would also like to thank *Dragos* and *DomainTools* for facilitating aspects of the above analysis. Finally, particular thanks to individuals who have assisted with this item, including but not limited to Amy Bejtlich, Casey Brooks, and several contributors who requested not to be recognized by name.

REFERENCES

- [1] MITRE. Group Dragonfly, Energetic Bear. 11 April 2021. <https://collaborate.mitre.org/attackics/index.php/Group/G0002>. [Accessed 08 June 2021].
- [2] MITRE. Dragonfly 2.0. 26 April 2021. <https://attack.mitre.org/groups/G0074/>. [Accessed 08 June 2021].
- [3] Greenberg, A. The Russian Hackers Playing Chekhov's Gun with US Infrastructure. *Wired*. 26 October 2020. <https://www.wired.com/story/berserk-bear-russia-infrastructure-hacking/>. [Accessed 08 June 2021].
- [4] 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>. [Accessed 08 June 2021].
- [5] Symantec. Dragonfly: Cyberespionage Attacks Against Energy Suppliers. 07 July 2014. https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers. [Accessed 08 June 2021].
- [6] Kaspersky Global Research and Analysis Team. Energetic Bear – Crouching Yeti. July 2014. <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf>. [Accessed 08 June 2021].
- [7] Meyers, A. Adversaries Set Their Sights on Oil and Gas Sector. *Crowdstrike*. 08 April 2015. <https://www.crowdstrike.com/blog/adversaries-set-their-sites-on-oil-and-gas-sector/>. [Accessed 08 June 2021].
- [8] Adobe. Security Advisory for Adobe Flash Player, Adobe Reader and Acrobat. 28 April 2011. <https://www.adobe.com/support/security/advisories/apsa11-02.html>. [Accessed 08 June 2021].

- [9] Kaspersky. Energetic Bear: More Like a Crouching Yeti. 31 July 2014. <https://securelist.com/energetic-bear-more-like-a-crouching-yeti/65240/>. [Accessed 08 June 2021].
- [10] Tacheau, E. Watering-Hole Attacks Target Energy Sector. 18 September 2013. Cisco Blogs. <https://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector>. [Accessed 08 June 2021].
- [11] Malwageddon. LightsOut EK: 'By the way... How much is the fish!?!'. 29 September 2013. <https://malwageddon.blogspot.com/2013/09/unknown-ek-by-way-how-much-is-fish.html>. [Accessed 08 June 2021].
- [12] Cisco Talos. Continued Analysis of the LightsOut Exploit Kit. 02 May 2014. <https://blog.talosintelligence.com/2014/05/continued-analysis-of-lightsout-exploit.html>. [Accessed 08 June 2021].
- [13] Cisco Talos. Hello, a New Specifically Covered Exploit Kit. 03 March 2014. <https://blog.talosintelligence.com/2014/03/hello-new-exploit-kit.html>. [Accessed 08 June 2021].
- [14] Hjelmvik, E. Full Disclosure of Havex Trojans. NETRESEC Network Security Blog. 27 October 2014. <https://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans>. [Accessed 08 June 2021].
- [15] Langill, J. T. Defending Against the Dragonfly Cyber Security Attacks. Belden. 22 October 2014. https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en. [Accessed 08 June 2021].
- [16] Peterson, D. Havex Hype & Unhelpful Mystery. 02 July 2014. <https://dale-peterson.com/2014/07/02/havex-hype-unhelpful-mystery/>. [Accessed 08 June 2021].
- [17] Wikipedia. MESA Imaging. 20 March 2020. https://en.wikipedia.org/wiki/MESA_Imaging. [Accessed 08 June 2021].
- [18] eWon. eWon Talk2M. <https://www.ewon.biz/cloud-services>. [Accessed 08 June 2021].
- [19] eWon. eWon eGrabit. <https://developer.ewon.biz/content/egrabit>. [Accessed 12 February 2020].
- [20] MB ConnectLine. MB ConnectLine mbCONNECT24. <https://www.mbconnectline.com/en/products/mbconnect24.html>. [Accessed 08 June 2021].
- [21] MB ConnectLine. Security Incident Follow-Up Report 09/19/2014. <https://www.mbconnectline.com/de/neuigkeiten/pressespiegel/detail/security-incident-follow-up-report-09192014.html>. [Accessed 07 February 2020].
- [22] Roberts, P. Industrial Control Vendors Identified in Dragonfly Attack. Security Ledger. 04 July 2014. <https://securityledger.com/2014/07/industrial-control-vendors-identified-in-dragonfly-attack/>. [Accessed 08 June 2021].
- [23] Cyphort. Windows Meets Industrial Control Systems (ICS) through HAVEX.RAT – It Spells Security Risks. 26 September 2014. <https://web.archive.org/web/20140926040520/https://www.cyphort.com/blog/windows-meets-industrial-control-systems-ics-havex-rat-spells-security-risks/>. [Accessed 08 June 2021].
- [24] Wilhoit, K. Havex, It's Down with OPC. FireEye. 17 July 2014. <https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html>. [Accessed 08 June 2021].
- [25] F-Secure. Havex Hunts for ICS/SCADA Systems. 23 June 2014. <https://archive.f-secure.com/weblog/archives/00002718.htm>. [Accessed 08 June 2021].
- [26] US CERT. ICS Advisory (ICSA-14-178-01). 22 August 2018. <https://www.us-cert.gov/ics/advisories/ICSA-14-178-01>. [Accessed 08 June 2021].
- [27] Hjelmvik, E. Observing the Havex RAT. NETRESEC Network Security Blog. 12 November 2014. <https://www.netresec.com/?page=Blog&month=2014-11&post=Observing-the-Havex-RAT>. [Accessed 08 June 2021].
- [28] Palo Alto Networks Unit42. Why Havex is a Game-Changing Threat to Industrial Control Systems – Part 1. 17 July 2014. <https://unit42.paloaltonetworks.com/havex-game-changing-threat-industrial-control-systems-part-1/>. [Accessed 08 June 2021].
- [29] US CERT. ICS Focused Malware (ICS-ALERT-14-176-02A). 22 August 2018. <https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-176-02A>. [Accessed 08 June 2021].
- [30] Haruyama, T. CB TAU Threat Intelligence Notification – Karagany Malware. Carbon Black. 12 August 2019. <https://www.carbonblack.com/blog/cb-tau-threat-intelligence-notification-karagany-malware/>. [Accessed 08 June 2021].
- [31] Constantin, L. New Malware Distribution Crimeware Kit Surfaces on the Underground Market/ 19 December 2010. Softpedia News. <https://news.softpedia.com/news/New-Malware-Distribution-Crimeware-Kit-Surfaces-on-the-Underground-Market-173591.shtml>. [Accessed 08 June 2021].

- [32] Bundesamt für Sicherheit in der Informationstechnik. Bericht zur Lage der IT-Sicherheit in Deutschland 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?jsessionid=0D0C277250AB9142211BC681A76B4043.2_cid341?__blob=publicationFile&v=2. [Accessed 08 June 2021].
- [33] Zetter, K. A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever. Wired. 08 January 2015. <https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>. [Accessed 08 June 2021].
- [34] Symantec. Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group. 20 October 2017. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>. [Accessed 08 June 2021].
- [35] US Cybersecurity and Infrastructure Security Agency (CISA). Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors. 20 October 2017. <https://us-cert.cisa.gov/ncas/alerts/TA17-293A>. [Accessed 08 June 2021].
- [36] US CISA. Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. 15 March 2018. <https://us-cert.cisa.gov/ncas/alerts/TA18-074A>. [Accessed 08 June 2021].
- [37] Nakashima, E. U.S. Officials Say Russian Government Hackers have Penetrated Energy and Nuclear Company Business Networks. Washington Post. 08 July 2017. https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfd9a2-638b-11e7-8adc-fea80e32bf47_story.html. [Accessed 08 June 2021].
- [38] SecureWorks Counter Threat Unit. Resurgent Iron Liberty Targeting Energy Sector. 24 July 2019. <https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector>. [Accessed 08 June 2021].
- [39] SpiderLabs. Responder. <https://github.com/SpiderLabs/Responder>. [Accessed 08 June 2021].
- [40] Baird, S.; Carter, E.; Galinkin, E.; Marczewski, C.; Marshall, J. Attack on Critical Infrastructure Leverages Template Injection. Cisco Talos. 07 July 2017. <https://blog.talosintelligence.com/2017/07/template-injection.html#more>. [Accessed 08 June 2021].
- [41] Perlroth, N. Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say. New York Times. 06 July 2017. <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html>. [Accessed 08 June 2021].
- [42] Hanson, R. Phishery. <https://github.com/ryhanson/phishery>. [Accessed 08 June 2021].
- [43] Smith R.; Barry, R. America's Electric Grid Has a Vulnerable Back Door – and Russia Walked Through It. Wall Street Journal. 10 January 2019. <https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112>. [Accessed 08 June 2021].
- [44] Klijnsma, Y. New Insights into Energetic Bear's Watering Hole Cyber Attacks on Turkish Critical Infrastructure. RiskIQ. 02 November 2017. <https://www.riskiq.com/blog/labs/energetic-bear/>. [Accessed 08 June 2021].
- [45] Kaspersky ICS CERT. Energetic Bear/Crouching Yeti: Attacks on Servers. 23 April 2018. https://ics-cert.kaspersky.com/media/EB_public_FINAL_EN_20042018.pdf. [Accessed 08 June 2021].
- [46] Slowik, J. Electric Sector Targeting in Context. Pylos. 26 December 2018. <https://pylos.co/2018/12/26/electric-sector-targeting-in-context/>. [Accessed 08 June 2021].
- [47] US CISA. Alert (TA18-106A) – Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices. 20 April 2018. <https://us-cert.cisa.gov/ncas/alerts/TA18-106A>. [Accessed 08 June 2021].
- [48] UK National Cyber Security Centre (NCSC). UK Internet Edge Router Devices: Advisory. 15 November 2018. <https://www.ncsc.gov.uk/information/uk-internet-edge-router-devices-advisory>. [Accessed 08 June 2021].
- [49] Lumen Black Lotus Labs. Newly Discovered Watering Hole Attack Targets Ukrainian, Canadian Organizations. 05 April 2021. <https://blog.lumen.com/newly-discovered-watering-hole-attack-targets-ukrainian-canadian-organizations/>. [Accessed 08 June 2021].
- [50] Cimpanu, C. Russian State Hackers Behind San Francisco Airport Hack. ZDNet. 14 April 2020. <https://www.zdnet.com/article/russian-state-hackers-behind-san-francisco-airport-hack/>. [Accessed 08 June 2021].
- [51] US CISA. Alert (AA20-296A) – Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets. 22 October 2020. <https://us-cert.cisa.gov/ncas/alerts/aa20-296a>. [Accessed 08 June 2021].
- [52] Perlroth, N. Russians Who Pose Election Threat Have Hacked Nuclear Plants and Power Grid. New York Times. 23 October 2020. <https://www.nytimes.com/2020/10/23/us/politics/energetic-bear-russian-hackers.html>. [Accessed 08 June 2021].
- [53] Kirkpatrick, D. D. British Cybersecurity Chief Warns of Russian Hacking. 14 November 2017. New York Times. <https://www.nytimes.com/2017/11/14/world/europe/britain-russia-cybersecurity-hacking.html>. [Accessed 08 June 2021].

- [54] Slowik, J. Conceptualizing a Continuum of Cyber Threat Attribution. Domain Tools. 02 March 2021. <https://www.domaintools.com/content/conceptualizing-a-continuum-of-cyber-threat-attribution.pdf>. [Accessed 08 June 2021].
- [55] Galeotti, M. Putin's Hydra: Inside Russia's Intelligence Services. European Council on Foreign Relations. https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf. [Accessed 08 June 2021].
- [56] UK NCSC. 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>. [Accessed 08 June 2021].
- [57] Microsoft Threat Intelligence Center. New Sophisticated Email-Based Attack Linked to NOBELIUM. 27 May 2021. <https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/>. [Accessed 08 June 2021].
- [58] Kaspersky ICS CERT. SunBurst Industrial Victims. 26 January 2021. <https://ics-cert.kaspersky.com/reports/2021/01/26/sunburst-industrial-victims/>. [Accessed 08 June 2021].
- [59] Slowik, J. The Enigmatic Energetic Bear. Pylos. 04 November 2020. <https://pylos.co/2020/11/04/the-enigmatic-energetic-bear/>. [Accessed 08 June 2021].
- [60] US Treasury Department. Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware. 23 October 2020. <https://home.treasury.gov/news/press-releases/sm1162>. [Accessed 08 June 2021].
- [61] FireEye. TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. 23 October 2018. <https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html>. [Accessed 08 June 2021].
- [62] Microsoft Defender Security Research Team. Analysis of Cyberattack on U.S. Think Tanks, Non-Profits, Public Sector by Unidentified Attackers. 03 December 2018. <https://www.microsoft.com/security/blog/2018/12/03/analysis-of-cyberattack-on-u-s-think-tanks-non-profits-public-sector-by-unidentified-attackers/>. [Accessed 08 June 2021].
- [63] Dunwoody, M.; Thompson, A.; Withnell, B.; Leathery, J.; Matonis M.; Carr, N. Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign. FireEye. 19 November 2018. <https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html>. [Accessed 08 June 2021].