

New Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East

By Limor Kessem

Published: 2019-12-04 · Archived: 2026-08-06 02:01:28 UTC

IBM X-Force has been researching and tracking destructive malware in the Middle East for some time now, particularly in the industrial and energy sectors. Since the first Shamoon attacks that started impacting organizations in the region in the summer of 2012, we have been following the evolution of destructive, disk-wiping malware deployed to cause disruption.

In a recent analysis, [X-Force Incident Response and Intelligence Services \(IRIS\)](#) discovered new malware from the wiper class, used in a [destructive attack](#) in the Middle East. We named this malware “ZeroCleare” per the program database (PDB) pathname of its binary file. To date, X-Force IRIS has not found any previous reporting on the ZeroCleare wiper, its indicators or elements observed in this campaign. It is possible that it is a recently developed malware and that the campaign we analyzed is one of the first to use this version.

According to our investigation, ZeroCleare was used to execute a destructive attack that affected organizations in the energy and industrial sectors in the Middle East. Based on the analysis of the malware and the attackers’ behavior, we suspect Iran-based nation-state adversaries were involved to develop and deploy this new wiper.

Given the evolution of destructive malware targeting organizations in the region, we were not surprised to find that ZeroCleare bears some similarity to the Shamoon malware. Taking a page out of the [Shamoon](#) playbook, ZeroCleare aims to overwrite the master boot record (MBR) and disk partitions on Windows-based machines. As Shamoon did before it, the tool of choice in the attacks is EldoS RawDisk, a legitimate toolkit for interacting with files, disks and partitions. The use of EldoS isn’t due to a flaw or [vulnerability](#) in that software. Nation-state groups and cybercriminals frequently use legitimate tools in ways that a vendor did not intend to accomplish malicious or destructive activity.

Using EldoS RawDisk with malicious intent enabled ZeroCleare’s operators to wipe the MBR and damage disk partitions on a large number of networked devices. To gain access to the device’s core, ZeroCleare used an intentionally vulnerable driver and malicious PowerShell/Batch scripts to bypass Windows controls. Adding these living-off-the-land tactics to the scheme, ZeroCleare was spread to numerous devices on the affected network, sowing the seeds of a destructive attack that could affect thousands of devices and cause disruption that could take months to fully recover from. These tactics resemble the way Shamoon was [launched in attacks](#) on Arabian Gulf targets in 2018.

Destructive Attacks Are a Rising Concern

X-Force IRIS has been following a marked increase in destructive attacks in the past year, having logged a whopping 200 percent increase in the amount of destructive attacks that our team has helped companies respond

to over the past six months (comparing IBM incident response activities in the first half of 2019 versus the second half of 2018).

[Destructive attacks on the energy](#) and industrial sectors have been a rising concern, especially in countries where the economy relies on oil and gas industries, like in some parts of the [Middle East and Europe](#). While we have seen them more frequently in the Middle East, these attacks are not limited to any part of the world and can be launched by any offensive nation-state group seeking to adversely affect the economy of rival countries, or by cybercriminals that use destruction as a pressure tactic.

The destructive attacks we have seen are being carried out by threat actors of varying motivations who could be employing destructive components in their attacks. Some pressure victims to pay them, others counterblow when they are not paid. When these attacks are carried out by nation-state adversaries, they often have military objectives that can include accessing systems to deny access to, degrade, disrupt, deceive or destroy devices and/or data.

ZeroCleare: A Complex, Targeted Attack

ZeroCleare attacks are not opportunistic and appear to be targeted operations against specific organizations. X-Force IRIS assesses that the ITG13 threat group, also known as [APT34/OilRig](#), and at least one other group, likely based out of Iran, collaborated on the destructive portion of the ZeroCleare attack. X-Force IRIS's assessment is based on ITG13's traditional mission, which has not included executing destructive cyberattacks in the past, the gap in time between the initial access facilitated by ITG13 and the last stage of the intrusion, as well as the different TTPs our team observed.

Infection Flow Basics

As the facilitator of the endgame of the attack, the ZeroCleare wiper is part of the final stage of the overall operation. It is designed to deploy two different ways adapted to 32-bit and 64-bit systems. The general flow of events on 64-bit machines includes using a vulnerable, signed driver and then exploiting it on the target device to allow ZeroCleare to bypass the Windows hardware abstraction layer and avoid some operating system safeguards that prevent unsigned drivers from running on 64-bit machines.

This workaround has likely been used because 64-bit Windows-based devices are protected with Driver Signature Enforcement (DSE). This control is designed to only allow drivers which have been signed by Microsoft to run on the device. Since ZeroCleare relies on the EldoS RawDisk driver, which is *not* a signed driver and would therefore not run by default, the attackers use an intermediary file named *soy.exe* to perform the workaround. They load a vulnerable but signed VBoxDrv driver, which the DSE accepts and runs, and then exploit it to load the unsigned driver, thereby avoiding DSE rejection of the EldoS driver.

Once loaded, the vulnerable VBoxDrv driver is exploited to run shellcode on the kernel level. Post-exploitation, the driver is used to load the unsigned EldoS driver and proceed to the disk wiping phase. Having analyzed *soy.exe*, we determined it was a modified version of the Turla Driver Loader (TDL), which is used to facilitate that very DSE bypass.

The same process does not apply to the 32-bit systems as they do not limit running unsigned drivers in the same manner.

Figure 1: ZeroCleared's top-level infection flow (Source: IBM X-Force)

The complete technical analysis of the [ZeroCleared malware attack](#) has been documented by X-Force IRIS researchers. You can also find ZeroCleared on [X-Force Exchange](#).

Attributing ZeroCleared: Possibly a Collaboration Between Iranian State-Sponsored Groups

X-Force IRIS assesses that the ZeroCleared campaign included compromise and access by actors from the [ITG13 group](#) and at least one additional group, likely Iran-based threat actors. Let's look at the details of some of the resources used throughout the ZeroCleared attack that can connect it with ITG13.

For initial access, the IP address `193.111.152[.]13`, which was associated with ITG13 in recent Oilrig/APT34 leaks and also reported by [Palo Alto Networks](#), was used to scan target networks and access accounts as early as fall 2018. A different Iranian threat actor likely accessed accounts from that address in mid-2019 preceding disk wiping operations.

One of the IP addresses used to access compromised network accounts in mid-2019 was `194.187.249[.]103`, which is adjacent to another IP address, `194.187.249[.]102`. The latter was used [several months prior](#) to the attack by the threat actor Hive0081 (aka [xHunt](#)). Additionally, while recent reporting from the [Cybersecurity and Infrastructure Security Agency \(CISA\)](#) indicated that the Russian threat actor IRIS tracks as [ITG12 \(aka Turla\)](#) had access to ITG13 tools and infrastructure potentially during this time frame, X-Force IRIS does not believe ITG12 was behind the ZeroCleared attack.

During the destructive phase, ITG13 threat actors brute-forced passwords to gain access to several network accounts, which were used to install the [China Chopper](#) and [Tunna](#) web shells after exploiting a SharePoint vulnerability. X-Force IRIS found an additional web shell named `extension.aspx`, which shared similarities with the ITG13 tool known as [TWOFACE/SEASHARPEE](#), including the methods that were dynamically called from assembly, the use of AES encryption and single-letter variable names.

The same threat actor also attempted to leverage legitimate remote-access software, such as TeamViewer, and used an obfuscated version of Mimikatz to collect credentials from compromised servers.

Regarding the ZeroCleared malware itself, while it shares some high-level similarities with Shamoon v3, specifically in how it uses an EldoS RawDisk driver, X-Force IRIS assesses that ZeroCleared is dissimilar enough in its code and deployment mechanism to be considered distinct from the Shamoon malware family and treated as separate malware.

While X-Force IRIS cannot attribute the activity observed during the destructive phase of the ZeroCleared campaign, we assess that high-level similarities with other Iranian threat actors, including the reliance on ASPX web shells and compromised VPN accounts, the link to ITG13 activity and the attack aligning with Iranian objectives in the region, make it likely this attack was executed by one or more Iranian threat groups.

Various links inferred from examining common TTPs and indicators of compromise as mentioned in the previous section make it possible that this wiper variant was built by Iran-based nation-state attackers. Recent activity from that sphere includes the Sakabota backdoor, recently reported by [X-Force IRIS](#) and also tied to ITG13, as well as the [Lyceum](#) campaign reported by Dell-EMC SecureWorks. In these campaigns, the top targets were Kuwaiti shipping and transportation organizations.

The Energy Sector in the Crosshairs

Nation-state attackers have typically carried out destructive attacks against the energy sector, with a historical focus on oil and gas companies; however, destructive attacks can target any entity. Why has this sector been finding itself in the crosshairs of such activity?

The key role oil and gas production and processing play on both the national and global level represents a high-value target for state-sponsored adversarial actors. These types of attackers may be tasked with conducting anything from [industrial espionage](#) to [cyber kinetic attacks](#) designed to disrupt the critical infrastructure of rival nations. Depending on the sophistication, scale and frequency of attacks, cyber incidents in this space have the potential to disrupt critical services, damage or destroy highly specialized equipment, and ultimately inflict detrimental cascading effects on [global energy security](#) and [industries downstream](#).

While nation-state attacks have been happening more in the past decade, it has been since at least 2012 that Iranian state-sponsored threat actors have been leveraging cyberattacks to inflict destructive, kinetic effects on their targets. The use of cyber-based weapons in lieu of conventional military tactics presents Iran, in this case, with a low-cost and potentially nonattributable means of conducting hostile and even warlike activities. With attribution to one specific group becoming a challenge nowadays, working under the cyber cloak of anonymity can also allow Iran to evade sanctions and preserve its relations with international players who may support its economic and nuclear energy interests.

Looking at the geographical region hit by the ZeroCleare malware, it is [not the first time](#) the Middle East has seen destructive attacks target its energy sector. In addition to underpinning the economies of several Gulf nations, the Middle Eastern petrochemical market, for example, hosts approximately 64.5 percent of the world's proven oil reserves, according to [OPEC](#), making it a vital center of [global energy architecture](#). Destructive cyberattacks against energy infrastructure in this arena, therefore, represent a high-impact threat to both regional and international markets.

Mitigating the Risk Posed by Destructive Malware

When it comes to destructive attacks, early detection and escalation as well as [coordinated response to contain and stop the spread of threats](#) are critical. Here are some tips from our team that can help mitigate the risk of destructive malware.

Use Threat Intelligence to Understand the Risk to Your Organization

Each threat actor has different motivations, capabilities and intentions, and [threat intelligence](#) can help provide insights that increase the efficacy of an organization's preparedness and eventual response to an incident.

Build Effective Defense-in-Depth

Incorporate multiple layers of security controls across the entire [Cyberattack Preparation and Execution Framework](#).

Figure 2: X-Force IRIS Cyberattack Preparation and Execution Framework (Source: IBM X-Force)

Deploy IAM, Limit Privileged Users and Implement MFA

In most attacks, adversarial actors leverage [privileged accounts](#) to expand their foothold in compromised networks. Limit the number of those accounts to a minimum and back them up with [multifactor authentication \(MFA\)](#). Don't allow one account to access all systems either.

Deploy [identity and access management \(IAM\)](#) to apply business-process-centric policies to what your users can access. That way, if their account is compromised, the attacker will have a harder time using it for access to other parts of the network. Leveraging IAM can also help baseline legitimate access and alert security teams when lateral movement could be abusing access to compromised accounts.

Have Backups, Test Backups and Keep Offline Backups

Backing up systems is a foundational best practice, but ensuring the organization has effective backups of critical systems and testing these backups is more important than ever. Being able to use backups in recovery can make a significant difference in remediating destructive malware attacks.

Test Your Response Plans Under Pressure

Using well-tailored tabletop exercises and [cyber range simulations](#) can help ensure that your teams are indeed ready, on both the tactical and strategic levels, to manage a destructive malware incident.

Rehearsed [response plans](#) require ongoing testing and adjustment, but they allow an incident response team to carry out plans and be able to implement them effectively when the time comes to respond and remediate.

For emergencies or if your organization is under attack, please call the IBM X-Force emergency response hotline at 1-888-241-9812 or (+001) 602-220-1440.

[Read the full X-Force report on the ZeroCleare wiper](#)

Source: <https://web.archive.org/web/20200211083637/https://securityintelligence.com/posts/new-destructive-wiper-zeroclare-targets-energy-sector-in-the-middle-east/>