Cybersecurity Threat Alert
Hackers of Savior
May 22, 2020

On May 21, 2020, a new hacktivist group going by the name ‘Hackers of Savior’ launched a defacing campaign targeting thousands of Israeli websites.

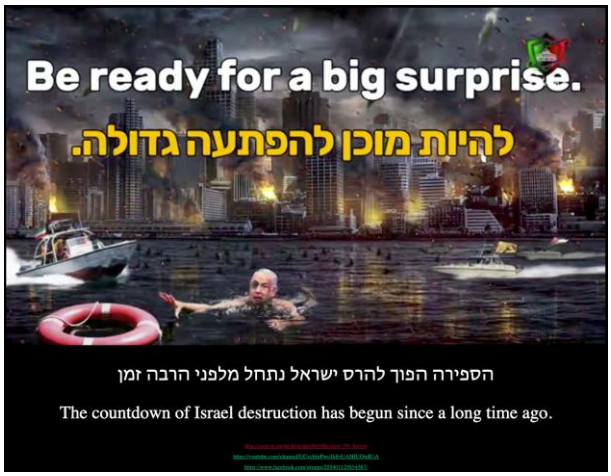

Figure 1: Defaced website

Background

There has been significant cyber activity over the previous two months leading up to the website defacing campaign. In April of 2020, Iran launched a cyberattack against Israel’s national water infrastructure. While no significant damage occurred, the cyberattack effected six facilities with impacts ranging from unauthorized access to data destruction. In retaliation, Israel launched a disruptive attack targeting Iran’s port facilities. This was followed by a warning from the Israel National Cyber Directorate in the middle of May about looming cyberattacks targeting Israel as part of the Anonymous operation #OpJerusalem and in association with the eve of Quds Day, an annual event held on the last day of Ramadan that was initiated by Iran in 1979.

The new website defacing campaign is being carried out by a new hacktivist group, Hackers of Savior, who formed on Facebook in April of 2020. At the time of publication, there is no indication that they are related to a nation state. On May 21, 2020, Hackers of Savior carried out what they called their ‘first step’ in targeting Israeli infrastructure and are using this attack as a platform to call for volunteers. Reports indicate that Hackers of Savior used a security vulnerability in a WordPress plugin to distribute their defacing exploits. A majority of the defaced websites were located on uPress, resulting in the vendor issuing a statement about the cyber event.

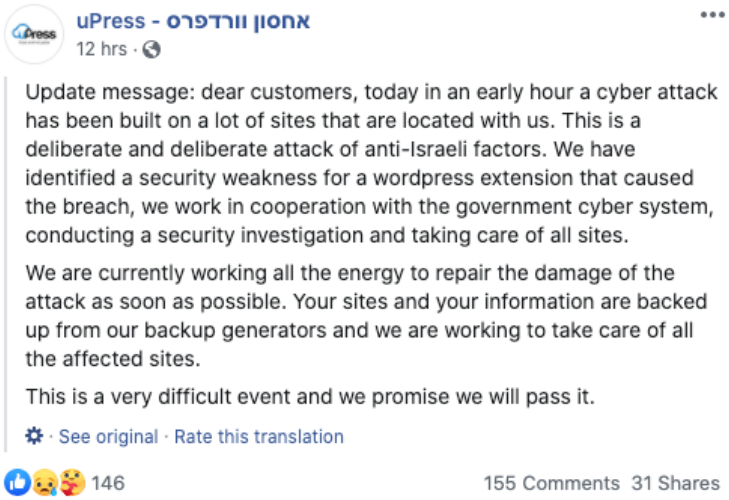

Figure 2: uPress post

The defaced websites showed a video and a countdown related to Quds Day. They also included links to social media pages run by Hackers of Savior. This defacement attack is indicative of previous cyberattacks launched by other groups in association with Quds Day.

Attack Methods

While exact details of the exploits used to breach the defaced websites are murky, available data indicates that WordPress-based websites hosted by uPress were compromised via a WordPress plugin.

Time	Notifier	H	M	R	L	★ Domain	OS	View
2020/05/21	Hackers_Of_Savior	H				[illegible]	F5 Big-IP	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H		R		[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior					[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Unknown	mirror
2020/05/21	Hackers_Of_Savior	H		R		[illegible]	Unknown	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H		R		[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H		R		[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H		R		[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H		R		[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior					[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror
2020/05/21	Hackers_Of_Savior	H				[illegible]	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Figure 3: List of unverified defacements by Hackers of Savior

Reasons for Concern

The group going by the name of 'Hackers of Savior' claim this is a first step to target Israeli infrastructure. While this group is considered a novice hacktivist group, they were able to find a common exploit in WordPress websites to maximize impact. While the primary aim was to spread propaganda, ZDNet notes that some sites loaded a script which requested access to a viewer's webcam and Radware researchers were able to verify this for a subset of the compromised websites.

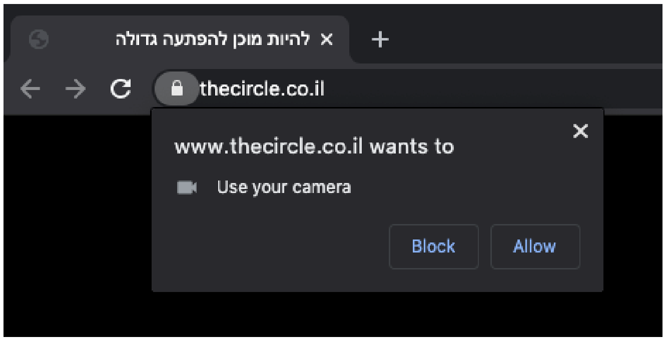

Figure 4: Request access to webcam

Conclusion

The administrator of the Hackers of Savior, which goes by the handle of Haloo Looya, called the defacing campaign “their first big surprise.” Expect the Hackers of Savior, and potentially other threat actors, to exploit the tensions between Israel and Iran over the coming days. These attacks will likely be linked to Quds Day or #OpJerusalem. When attributing these attacks, caution should be exercised to avoid attributing them to Israeli or nation state operators.

Figure 5: Hackers of Savior administrator

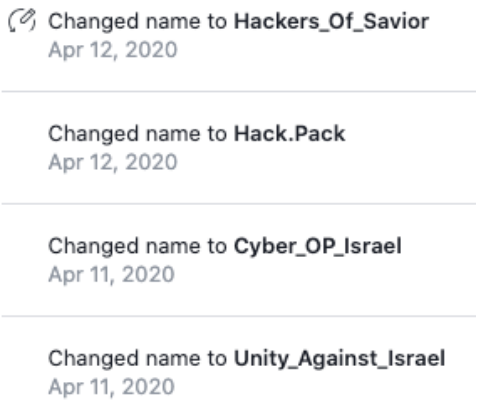

Figure 6: Facebook Group name changes

Figure 7: Hackers of Savior Logo

References

YouTube - https://www.youtube.com/channel/UCycbfgPwo1k8vUAHfUQmR1A
Facebook - https://www.facebook.com/groups/255401125854567/
Twitter - https://twitter.com/jOCKER71080226
Embedded Video Link - https://streamable.com/e/lt1z11
Email - HackersOfSavior@gmail.com

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** - using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.