HERJAVEC GROUP

Threat Landscape Developments

2021 State-Sponsored Cyber Activity

HERJAVEC GROUP

Threat Landscape Developments

Overview

The state of the global threat landscape has continued to shift through 2021. Cyber-attacks against enterprises like Colonial Pipeline and JBS South America caused disruption and downtime that had a cascading effect on many industries and organizations. With some of the largest and most damaging ransomware attacks occurring this year, it's no wonder law enforcement agencies have begun aggressively pursuing threat actors, taking an offensive approach to dealing with cybercrime.

Today, the threats we face are sophisticated, global, and in many cases, backed by nation states. This year, threat intelligence related to cyber-operations has been observed by the nation-states of Iran, China, Russia, and North Korea. This activity continues to dominate the threat landscape of Western governments and organizations.

In the 2021 State-Sponsored Cyber Activity Report, Herjavec Group's Threat & Vulnerability Management Team have analyzed the evolving global threat landscape in 2021 and reported on law enforcement countermeasures, threat actor responses to countermeasures, state-sponsored cyber threats, and the global impact of Israeli-based NSO Group's mobile device spyware, *Pegasus*.

Contents

2021 Law Enforcement Countermeasures

Disruptions and Shutdowns

January: Europol announces that a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, Ukraine, Europol and Eurojust successfully disrupted *Emotet* [1].

Department of Justice announces that a joint operation between Canadian and American authorities results in the seizure and shutdown of NetWalker Ransomware's infrastructure [2].

February: *Egregor*'s network, including their extortion site and C2 infrastructure go offline [3].

April: FBI personnel gain authorization to search the compromised Microsoft Exchange Servers and, through interactions with the web shells, uninstall the web shells on those servers [4].

May: Following the *Colonial Pipeline* ransomware attack, *Darkside Ransomware* infrastructure goes offline [5].

July: All of *REvil*'s infrastructure, including their data leaks site disappears and goes offline [6]–[8].

November: *BlackMatter Ransomware Group* announces they are closing their operations, cites "mounting pressure from law enforcement" [9].

Cryptocurrency Recovery

January: Department of Justice announces that $454,530.19 in cryptocurrency was seized during a joint operation between Canadian and American authorities to shutdown *NetWalker Ransomware* [2].

July: Department of Justice announces the seizure of 63.7 Bitcoins (BTC), which was approximately $2.3 million USD at the time. Attributes the funds as a portion of the "proceeds of a May 8 ransom payment to individuals in a group known as *DarkSide*" [10].

Arrests and Indictments

January: Quebec resident and Canadian national is indicted by the Middle District of Florida for alleged *NetWalker Ransomware* association [2].

February: France's public News Radio station is the first to disclose the arrest of Egregor *(Maze Hacking Team)* ransomware affiliates by Ukrainian Law enforcement [11].

September: South Korea's national police agency's cybersecurity investigation bureau announces the arrest of suspected *REvil/GandCrab* affiliate [12].

November: Two *REvil* ransomware suspected affiliates arrested by Romanian authorities. On the same day, Kuwaiti authorities also arrest a suspected *GandCrab* affiliate [13].

Timeline of various major law enforcement events in 2021

January
Emotet infrastructure disrupted

February
Egregor affiliates arrested

February
Egregor infrastructure goes offline

April
FBI granted court-order to remediate compromised Exchange Servers

May
Darkside Ransomware infrastructure goes offline

July
Department of Justice announces seizure of 63.7 Bitcoins allegedly attributed to Darkside operations

July
REvil silently goes offline

October
After resurging in September, REvil offline once more; Law enforcement allegedly compromised REvil before their last known good backup

November
BlackMatter shutting down, cites "mounting pressures from law enforcement"

November
Two arrested in Romania, allegedly related to REvil

Threat Actor Responses to Countermeasures

In May 2021, the now-defunct *DarkSide Ransomware Group* successfully ransomed *Colonial Pipeline* for $11M (USD) [14]. In the same month, *REvil* successfully executed a ransomware attack on JBS South America - a Brazilian-based global supplier of beef and pork products. REvil followed this attack up with another massive attack in July on Managed Service Providers (MSPs) supplying remote monitoring and management services via Kaseya's Virtual System Administrator (VSA) software platform.

In a coordinated response led by the American government and Five-Eyes associated nation-states, a rapid, effort to disrupt ransomware-actor operations began. During the counter-operation, authorities were able to seize both Darkside and REvil's operational infrastructures and recover millions of dollars-worth of Convertible Virtual Currency (CVC). Some key ransomware affiliates reacted by retiring operations, as seen by *REvil's 0_neday*:

THE SERVER WAS COMPROMISED, AND THEY WERE LOOKING FOR ME. TO BE PRECISE, THEY DELETED THE PATH TO MY HIDDEN SERVICE IN THE TOR.RC FILE AND RAISED THEIR OWN SO THAT I WOULD GO THERE. I CHECKED ON OTHERS – THIS WAS NOT. GOOD LUCK EVERYONE, I'M OFF.

This is likely only a brief reprise from operations in order to retool Operational Security (Op-Sec) before re-emerging with a new campaign. This is a commonly witnessed maneuver that has already been observed by sophisticated threat actors such as *Indrik Spider*, *Prometheus Ransomware*, and *DarkSide Ransomware* in the past [15], [16].

However, not all threat actors appear deterred by the increase in counter-operations. Instead, many cyber criminal syndicates appear galvanized by the actions taken by the government. In response, these actors have showed increased solidarity, socio-political involvement, and acknowledgement of each other's respective operations. Many groups have contacted Western Media sources directly and published disparaging 'publicity statements' which openly ridicule counter-operation efforts, branding law enforcement initiatives as ineffective and hopeless.

By far, the strangest attempt to sow discord and discredit counter-efforts was observed by the fictious *"Groove Ransomware"* group. To this date *Groove Ransomware* has never claimed any victims. Instead, the actor(s) behind this group invested their time and resources into manipulating Western media, cheerleading on behalf of other groups, and encouraging Russian ransomware operators to seek out affiliations with Chinese cyber attackers as a punishment against Western civilizations.

"

By the way, the headlight wished that I was offended in the gill, so that's what I want to tell you about: I had an idea to check whether it is possible to manipulate the media (large) through the Rans blod. I have checked and it is possible. Groove gang does not exist - this is a kind of trolling of the Western media and it once again shows how they are afraid of us. In general, manay people know me from the damage lab aka xss forum, I sometimes write articles there, help newbies rise in this area. Not so long ago I decied to write an article "Manipulation of the media through ranso blog", I needed a groove only for this. And I was good at manipulating the media. Yes indeed all the information that I described here was real.

- Groove Ransomware; statement regarding legitimacy

State Specific Activity

The Islamic Republic of Iran

Since September 2020, Iranian threat-actors' have continue to evolve their *Tactics*, *Techniques*, and *Procedures (TTPs)*. When compared to the latter half of the previous decade, in 2021, state-sponsored Iranian threat-groups have demonstrated increased maturity with regards to successfully accomplishing mission objectives. Not only are cyber attacks more frequent, Iran has been observed conducting suspected state-sponsored ransomware operations, likely to fund other cyber operations [17].

Furthermore, Herjavec Group's Threat & Vulnerability Management team has observed the maturation of Iranian state-sponsored activity: When compared against historical operations, Iranian state-sponsored actors have demonstrated increased patience post-initial access to avoid detection when compared to their previous campaigns. Finally, according to Microsoft's Threat Intelligence Center (MSTIC), Iranian threat-actors have been observed following a common trend in the threat landscape this year, a dramatic increase of using brute-force attacks **(T1110 – Brute Force)** to acquire credentials for usage in additional to traditional mal-spam based spear-phishing campaigns **(T1566 – Phishing)**[17]. The following (see next page) is a timeline of Iranian nation-state threat actors, observed throughout 2021.

PHOSPHORUS has been observed to aggressively scanning millions of IPs to look for vulnerable Fortinet FortiOS SSL VPN (CVE-2018-13379), and has exploited the vulnerable Fortinet systems, as well as unpatched on-premises Exchange Servers globally to deploy ransomware **(T1190 - Exploit Public Facing Application)**. PHOSPHORUS has also deployed BitLocker-based **(T1587.001 - Develop Capabilities: Malware)** ransomware to extort victims **(T1486 - Data Encrypted for Impact)**. In 2021, PHOSPHORUS invested increasing amounts of time and resources to build extensive connections with their victims before targeting them **(T1585 - Establish Accounts)** before following up with more aggressive techniques to initiate the attack chain. In some instances, PHOSPHORUS has been observed contacting targets several times a day in order to get response [17] **(T1598 - Phishing for Information)**.

CURIUM is another threat-actor whose operations appear to be aligned with furthering Iranian interests [17]. CURIUM uses fake social media accounts to build a rapport with targets before delivering malware over the social platform **(T1566.003 – Phishing: Spearphishing via Service)**. The group has used other people's pictures on social media as their profile images **(T1585.001 - Establish Accounts: Social Media Accounts)**, particularly of women. CURIUM actors have shown extended amounts of patience when disarming their targets. After a good relationship is established, they will finally send malicious files, requesting their victim open them for fictitious reasons **(T1204.002 – User Execution: Malicious File)**.

DEV-0343, is the name given by Microsoft for another Iranian threat group that has been extremely active throughout 2021. Using official red-team testing tools such as *Cobalt Strike*, DEV-0343 leverages brute force attacks **(T1110 - Brute Force)** and password

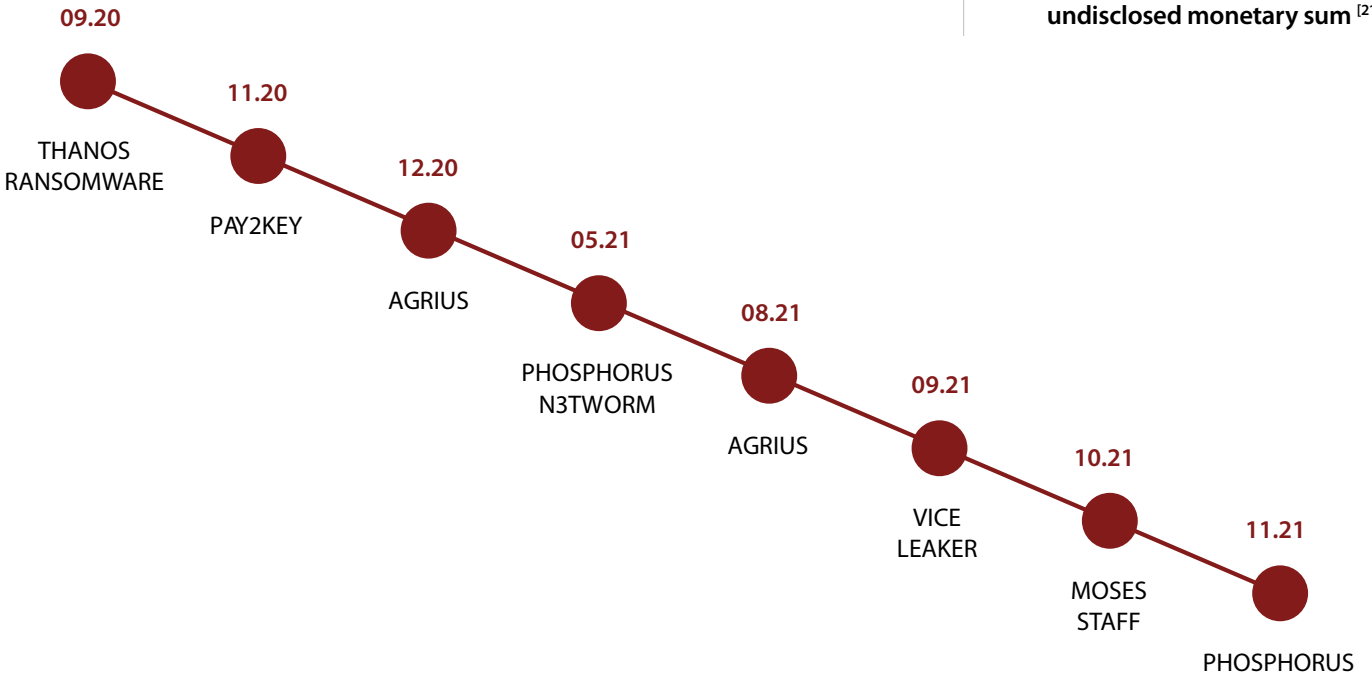
spray attacks **(T1110.003 - Brute Force: Password Spraying)** to aggressively target Azure Office 365 tenants [17]. Targets in these attacks have included defense companies supporting US, EU, and Israeli governments, customers of Persian Gulf-related geographic information systems (GIS) & spatial analytics services, as well as several maritime and cargo transportation companies primarily operating within the Middle East [17].

As of autumn 2021, a suspected politically motived threat-group named **Moses Staff** began repeatedly launching attacks on Israeli targets. After successfully compromising target networks Moses Staff exfiltrates corporate secrets and other sensitive information, followed by attempting to irreparably tamper with victim data **(T1485 - Data Destruction)** and impede continued operations. At the time of this publication, Moses Staff, has yet to demand a ransom from its victims, and has released the exfiltrated data of its victims free [18].

All of the aforementioned activity in 2021 demonstrates Iranian nation-state threat actors are maturing their operations and investing resources into developing a wide variety of attacks including ransomware, destructive, disk-wiping malware, long-term covert espionage campaigns, and software supply chain infiltration **(T1195.003 - Supply Chain Compromise: Compromise Software Supply Chain)**.

Iranian Counterintelligence

On November 4th 2021, Omri Goren Gorochovsky, a cleaner working in the home of Israeli Defense Minister Benny Gantz, was arrested for allegedly offering to spy for BlackShadow [19], a hacking group attributed with being an Iranian state-sponsored hacking group with confirmed links to Pay2Key Ransomware operations [20]. Gorochovsky is suspected of initiating contact with Black Shadow via the encrypted messaging platform, Telegram, and sending photos of different items from Gantz's house such as pictures of his desktop computer, cellphone, and tax documents. Gorochovsky is suspected of telling a BlackShadow representative that he was willing to infect the minister's computer for an undisclosed monetary sum [21].



People's Republic of China

China has a notoriously long-held history of state-sponsored offensive cyber-operations in the interest of furthering Chinese national interests. In July 2021, the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) published Alert AA21-200B, asserting "The National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China state-sponsored malicious cyber activity is a major threat to U.S. and Allied cyberspace assets", and then detailed the observable TTPs associated with Chinese State-Sponsored cyber operations [22].

In 2021, Chinese state-sponsored cyber operations have demonstrated an agile approach to acquisition of infrastructure and capabilities **(T1583.006 - Acquire Infrastructure, T1588 – Obtain Capabilities)**, showing threat-actor cognizance of how to play the continued cat-and-mouse game between infiltrators and defenders. In 2021, Chinese state-sponsored actors commonly obfuscated their true location via the revolving usage of Virtual Private Servers (VPS) **(T1583.003 – Acquire Infrastructure: Virtual Private Server)** and compromised small office and home office (SOHO) **(T1584 - Compromise Infrastructure)** devices as encrypted multi-hop proxy nodes **(T1573 – Encrypted Channel, T1090.003 - Proxy: Multi-Hop Proxy)**

In 2021, Chinese State-sponsored groups have been observed creating chains of zero-days and weaponizing new vulnerabilities within days of them being publicly disclosed. These groups primarily have focused on major applications such as Pulse Secure VPN, Apache Struts, F5's Big-IP **(T1190 - Exploit Public Facing Application)**, Microsoft Exchange Server, and Microsoft's Objecting Linking and Embedding (OLE) technologies **(T1203 - Exploitation for Client Execution)** [23]–[25]. Furthermore, these groups have outfitted their operations with a combination of open-source and commercial penetration **(T1588.001 - Obtain Capabilities: Tool)** tools to evade fingerprinting themselves with custom malware during their campaigns.

During March 2021, researchers from Volexity and Microsoft discovered the active exploitation of multiple previously undiscovered Microsoft-exchange vulnerabilities by a group named **HAFNIUM**. HAFNIUM is a geopolitically motivated group which primarily targets organizations and individuals in the United States working as defense contractors, conducting infectious disease research, relating to law and government, higher-education, and foreign-policy think-tanks or Non-Governmental Organizations (NGOs) [27, Sec. Who is HAFNIUM?]. The attackers weaponized a server-side request forgery (SSRF) vulnerability in on-premises instances of Microsoft Exchange Server **(T1212 - Exploitation for Credential Access)**, followed by the exploitation of an insecure deserialization vulnerability which elevated HAFNIUM to SYSTEM level on the Exchange server. After securing SYSTEM level permissions, HAFNIUM used arbitrary file-write vulnerabilities to deploy ASP web-shells **(T1505.003 - Server Software Component: Web Shell)** on the impacted exchange servers [26], [27].

Meanwhile, in the summer of 2021, a cluster of threat activity known as Threat Activity Group 22 (TAG-22), which Recorded Future's *Insikt Group* assesses to be another state-sponsored Chinese group was observed targeting telecommunications, academia, research and development, and government institutions in Nepal, the Philippines, Taiwan, and Hong Kong [28]. During these attacks, this group, also known as Winnti Group was observed [29], [30] using compromised Glassfish servers **(T1584.004 - Compromise Infrastructure: Server)** and Cobalt Strike to facilitate Initial Access, before deploying the custom Winnti, and ShadowPad backdoors [28].

The Russian Federation

Ghostwriter is the Mandiant-given name for a series of information and influence operations which have been on-going since at least March 2017 and appear to be aligned with Russian security interests [31]. According to *Mandiant, Ghostwriter* operations have historically targeted audiences in Lithuania, Latvia, and Poland with narratives critical of the North Atlantic Treaty Organization's (NATO) presence in Eastern Europe, as well as spreading other anti-American and anti-NATO sentiment. Between October 2020 and January 2021, *Ghostwriter* was observed compromising the social media accounts of Polish officials **(T1586.001 - Compromise Accounts: Social Media Accounts)**, using legitimate news websites **(T1584.001 - Compromise Infrastructure: Domains)** to publish fabricated content, and send messages via spoofed variants of the emails of legitimate public figures **(T1585.002 – Establish Accounts: Email Accounts)** with intention to discredit the Polish government and exacerbate political division within the country [31], [32].

Russia-Belarus Relations

In April 2021, *Mandiant Threat Intelligence* released an updated report on *Ghostwriter* campaigns. In this update, *Mandiant*'s researchers assess with high confidence that a threat actor, now independently being tracked as UNC1151, "is a state-sponsored cyber-espionage focused group that engages in credential harvesting, malware campaigns and [is responsible for conducting] at least some components of *Ghostwriter* influence [operations]" [32, p. 4]. Throughout these springtime campaigns, UNC1151 demonstrated interest in activities relating to the ongoing discussions revolving around the potential of the Russian-Belarusian merging of political and economic affairs [33].

As of November 2021, *Mandiant Threat Intelligence* researchers have expressed that they have not been able to conclusively determine if UNC1151 is a Russian state-sponsored actor, Belarusian threat-actor, or an overlap of both, due to the intersecting geopolitical goals of both nation states [34].

Secondary Infektion

Like *Ghostwriter, Secondary Infektion* is another threat-actor-supported misinformation campaign suspected of having Russian-based origins. According to *Recorded Future's Insikt Group*, this threat actor has been operational since at least 2014. As seen with *Ghostwriter,* an emphasis on hardened Op-Sec measures prevented *Insikt Group* from definitively attributing *Secondary Infektion* activity to a previously defined Russian threat-actor [35].

In 2021, *Secondary Infektion* compromised a waves of disinformation blog posts, submitted by burner personas on blogging websites and the popular social media platform Reddit **(T1585.001 - Establish Accounts: Social Media Accounts)**.

Furthermore, during 2021, *Secondary Infektion* was also observed by *Recorded Future*'s *Insikt Group* conducting campaigns where burner personas were used to fictitiously conduct operations on behalf of *Anonymous Kazakhstan*. In these campaigns, the group was observed continuing to attempt to "sow mistrust of Sweden's political figures domestically, [and] create uncertainty and false optimism among Ukrainians, [in order to] shape negative perceptions of NATO, Ukraine [and Sweden] among Russian audiences" [36].

Russian Counterintelligence

On September 28th, 2021, Russian Security Firm Group IB 's CEO and founder Ilya Sachkov, was arrested by Russian Authorities in Moscow. Ilya is being charged under Article 275 of the Russian Criminal Code on state treason charges for the "transfer of classified information to foreign agencies which allegedly "employed" the executive" [37],[38]. Russian law enforcement agencies had raided Group-IB's Moscow office, however, Group-IB continued to operate as normal due to decentralized structure of their business and operations. [39]. An official statement from Group-IB states Ilya has not admit guilt to these charges and maintains his innocence [37]. Ilya in the past had been observed to be critical in regards to the Russian government and its lack of expediency apprehending Russian cyber criminals [38].

The Democratic People's Republic of Korea

The North Korean government—officially known as the Democratic People's Republic of Korea (DPRK)—is another nation-state that has long-employed state-sponsored cyber activity with the interest of furthering DPRK-related national interests. This has included cyber-espionage, bank/SWIFT theft, and ransomware attacks **(T1486 – Data Encrypted for Impact)** in the interest of generating revenue, in addition to destructive data attacks **(T1485 – Data Destruction)**.

Intelligence reveals DPRK continues to conduct its cyber operations worldwide with a growing appetite for targets. Many of DPRK's well known cyber-actors, such as *Andariel, Bluenoroff, Kimsuky, Lazarus, Reaper*, and *ScarCruft* operate under the direction of its *Reconnaissance General Bureau (RGB)*. The RGB is suspected of using proceeds from financially motivated campaigns to raise funds for North Korea's Weapons of Mass Destruction (WMD) programs. According to confidential reporting from the United Nations obtained by *Reuters*, DPRK has funded approximately two billion USD through illicit cyber-activity [40] for this program.

DPRK's threat actors combine the usage of credential harvesting **(T1589.001 – Gather Victim Identity Information: Credentials)** and spear-phishing campaigns using *SendGrid* **(T1566.003 – Phishing - Spearphishing via Service, T1566.002 Spearphishing Link)**, malicious browser extensions **(T1176 - Browser Extensions)**, HTA-based malware **(T1218.005 - Signed Binary Proxy Execution: Mshta file)**. The malicious executable is obfuscated with null-byte padding **(T1027 - Obfuscated Files or Information: Binary Padding)**, .7z compression **(T1140 - Deobfuscate/Decode Files or Information)**, and being UPX-packed malicious executable **(T1027.002 - Obfuscated Files or Information: Software Packing)** to impede analysis efforts [41].

Threat intelligence produced by ProofPoint in autumn 2021 highlights that DPRK-related threat-groups have increased their attack volume to "almost weekly" campaigns, using themes such as nuclear weapon safety, President Joe Biden, Korean foreign policy and other political themes to phish desired targets within foreign policy, journalism, academia, law enforcement agencies, financial institutions, and nongovernmental organizations. Additionally, DPRK orchestrated adversaries have expanded standard targeting to include financially motivated campaigns involving cryptocurrency fraud, and sexual extortion ('sextortion') schemes.

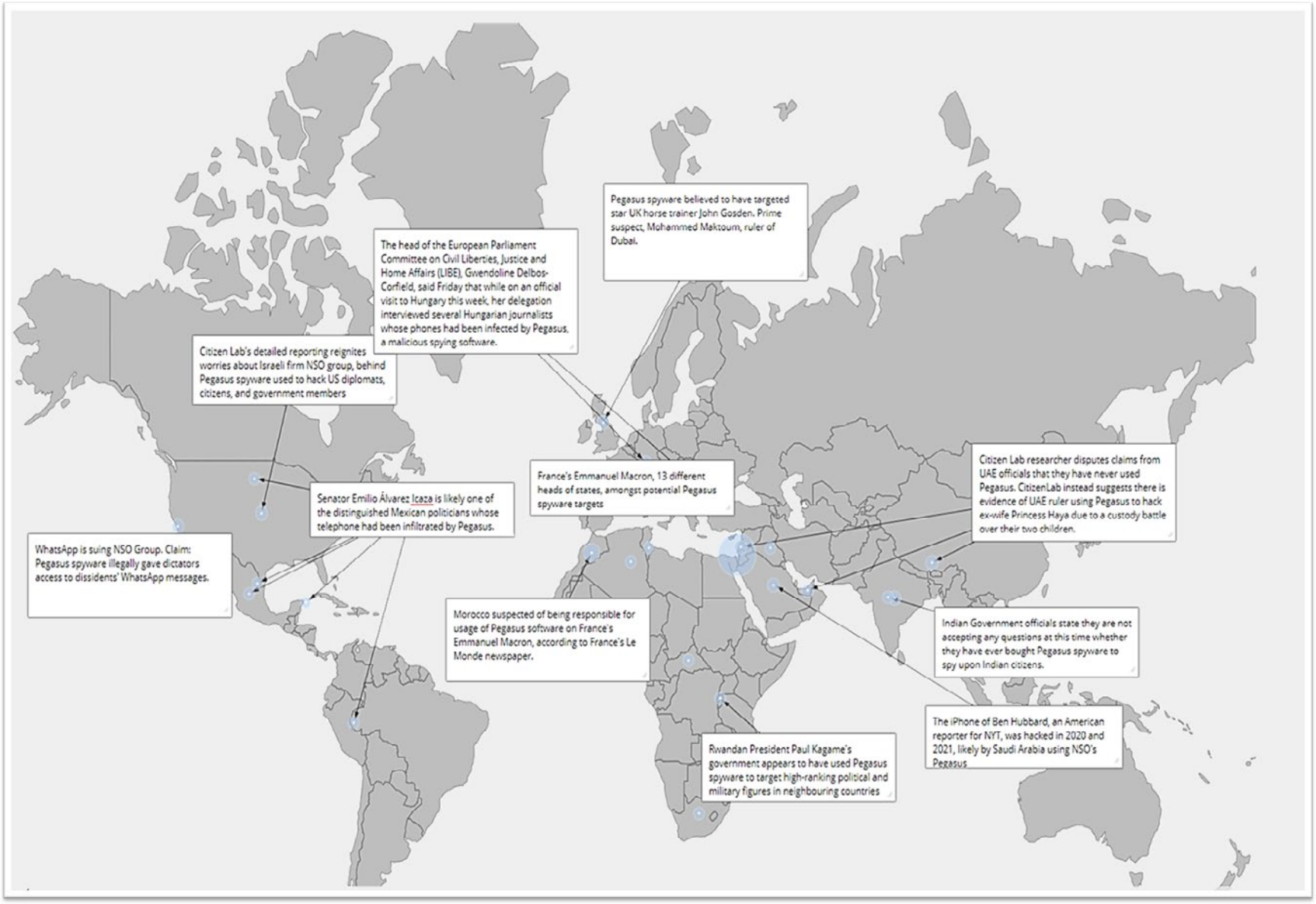
NSO Group & Pegasus Spyware

NSO Group is an Israeli-based, commodity cyber-warfare software vendor. They are most notorious for their mobile-phone spyware suite *Pegasus*. Researchers at *The Citizen Lab* of *University of Toronto's Munk School of Global Affairs and Policy* first brought attention to *Pegasus* and *NSO Group* in 2018 when they publicly disclosed that between August 2016 and August 2018 they "found 1,091 IP addresses matching [Pegasus's fingerprint] and 1,014 domain names that pointed to [the IP addresses]" with active operations in over 45 countries [42].

Simultaneously in 2018, *NSO Group* was further thrust into the global spotlight after forensic analysis experts determined that the phones of *The Washington Post* journalist Jamal Khashoggi, and those close to him, demonstrated evidence of Pegasus software infections between 2017-2018. The forensic evidence demonstrates that the espionage continued on these devices even after his murder [43]. Even further, it was also discovered that as an attempt to infect Khashoggi, MBS personally delivered the zero-click malware to Jeff Bezos personal phone number using WhatsApp. MBS then used this access to uncover and leak nude photographs of Jeff Bezos, publicly exposing the extramarital affair he later admitted he was having at that time [44].

Three years later, *NSO Group* continues to maintain that they do not have government officials in their customer-base, something which does not align with the continued investigation conducted by The Citizen Lab released throughout 2021. Instead, *The Citizen Lab* researchers uncovered usage of novel iOS exploits being used by Pegasus's growing customer base. The breadth of the NSO Group's customer-base highlights a paradigm shift in cybersecurity, where not only government organizations and global enterprises are a target. In fact, some *The Citizen Lab*'s reporting even suggests that some of *NSO Group*'s customers may be using Pegasus to illegally spy on their own citizens [45]–[47].

Global Impact of 2021



Conclusion

The HG Threat Team suggests the following to deal with active incidents and prevent further breaches:

When responding to an active infection:

- First, disrupt any active infections by removing the infected device from the network until it can be re-imaged or cleaned. Unplug device's the network cable or turning the device off altogether.
- Leverage your proactive resources. Restore data from back-ups and re-image the infected devices. Re-image the device from known-good images, to eliminate not only the detected ransomware but any other malware that may have been downloaded at the same time.
- Eradicate the source of the infection. If you suspect that the malware was delivered via email, it may be useful to find the source email and delete it from all mailboxes to prevent reinfections. · Be proactive and prepared. Have an Incident Response team on retainer so they can step in and respond in the most effective and efficient way during an active infection.
- Be proactive and prepared. Have an Incident Response team on retainer so they can step in and respond in the most effective and efficient way during an active infection.

AS THE GLOBAL THREAT LANDSCAPE CONTINUES TO EVOLVE, IT IS CRITICAL FOR ENTERPRISES AND INDIVIDUALS ALIKE TO DO THEIR PART IN PREVENTING CYBERCRIME. NOW IS THE TIME TO IMPLEMENT BEST PRACTICES FOR CYBER DEFENSE, CONTINUOUSLY IMPROVE YOUR CYBERSECURITY POSTURE, AND BE PREPARED TO RESPOND QUICKLY AND EFFECTIVELY TO ANY BREACHES THAT MAY OCCUR.

To further prevent cybercrime breaches in the future:

- Deploy advanced web and email gateway protection.
- Implement advanced endpoint protection including behavior driven analysis. Ensure your endpoint protection examines traffic for behaviors, rather than just file-matching.
- Block potential adversary threat vectors such as adware, known bad domains (blacklists for C2 servers), and unknown/unclassified domains by leveraging web content filtering appliances or firewall features. While this can cause minor impacts to business, being intentional about which appliances and firewall features you implement will generally only result in tolerable restrictions.
- Deploy a Microsoft Group Policy to restrict software's ability to run from %appdata% and "temp" folders. These are generally used by malware because all users have the ability to write to these locations predictably, and permission cannot be restricted without affecting system function. However, there are few-to-none reasons why software should install or have to run from these directories. If the malware can't run, it can't do any harm.
- Restrict web browsing and email use by privileged users such as administrators. Have separate accounts for administration and day-to-day computing.
- Implement Privileged Access Management best practices. Minimize the permissions to network file shares. Give the ability to write/modify files only to the users that require it, and only to the necessary locations.
- Carry out a policy that no corporate information should be stored on local hard drives, USB drives, or other local storage. Files stored on the network are normally backed up and can be restored with minimal disruption to the business. · Educate the people using your devices on how to recognize spam and phishing emails and what to do if they receive it.
- Prepare for the worst, and have an Incident Response plan ready. The worst time to decide what to do about an attack is after it has occurred. If your organization doesn't already have one, we suggest using the 10 Point IR Plan laid out in the Cybersecurity Conversations for the C-Suite Report as a blueprint to developing one that fits your organization's needs.

HERJAVEC GROUP

Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. We have expertise in comprehensive security services, including Advisory Services, Technology Architecture & Implementation, Identity & Access Management, Managed Security Services, Threat Hunting & Management, Digital Forensics and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, Canada and India.
For more information, visit HerjavecGroup.com or contact us at info@herjavecgroup.com.

References

[1] Europol, "World's most dangerous malware EMOTET disrupted through global action | Europol," Europol, Jan. 2021. Accessed: Nov. 18, 2021. [Online]. Available: https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[2] Wednesday, January 27, 2021, "Department of Justice Launches Global Action Against NetWalker Ransomware," Jan. 27, 2021. https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware (accessed Nov. 22, 2021).

[3] C. Cimpanu, "Egregor ransomware operators arrested in Ukraine," ZDNet, Feb. 14, 2021. https://www.zdnet.com/article/egregor-ransomware-operators-arrested-in-ukraine/ (accessed Nov. 18, 2021).

[4] SOUTHERN DISTRICT OF TEXAS, HOUSTON DIVISION, MOTION TO PARTIALLY UNSEAL SEARCH WARRANT AND RELATED DOCUMENTS AND [PROPOSED] ORDER. 2021. Accessed: Nov. 18, 2021. [Online]. Available: https://www.justice.gov/opa/press-release/file/1386631/download

[5] "Darkside ransomware gang says it lost control of its servers & money a day after Biden threat," The Record by Recorded Future, May 14, 2021. https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/ (accessed Nov. 18, 2021).

[6] vx-underground, "@LawrenceAbrams REvil representative, Unknown, has not said anything on Exploit or XSS since July 8th.," @vxunderground, Jul. 13, 2021. https://twitter.com/vxunderground/status/1414936692516171779 (accessed Nov. 18, 2021).

[7] L. Abrams, "Lawrence Abrams on Twitter: 'Plot thickens. "Support staff is offline" https://t.co/aqjxSUpnDg' / Twitter." https://twitter.com/LawrenceAbrams/status/1414989417232601094 (accessed Nov. 18, 2021).

[8] "@LawrenceAbrams REvil representative, Unknown, has not said anything on Exploit or XSS since July 8th.," Twitter. https://twitter.com/vxunderground/status/1414936692516171779 (accessed Nov. 18, 2021).

[9] C. Page, "BlackMatter ransomware gang says it's shutting down over law enforcement pressure | TechCrunch," Nov. 03, 2021. https://techcrunch.com/2021/11/03/blackmatter-ransomware-shut-down/ (accessed Nov. 22, 2021).

[10] "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," Jun. 07, 2021. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (accessed Nov. 18, 2021).

[11] E. Leclère, "Cybersécurité : des pirates 'Egregor', à l'origine de l'attaque contre Ouest-France, interpellés en Ukraine," France Inter, Feb. 12, 2021. https://www.franceinter.fr/amp/justice/cybersecurite-des-pirates-egregor-a-l-origine-de-l-attaque-contre-ouest-france-interpelles-en-ukraine (accessed Nov. 18, 2021).

[12] Y. Hee-Gon, "'□□□□□□□□□□□□' □□□□□□ 20□□□□ 20□□□□," □□□□, Mar. 09, 2021. Accessed: Nov. 22, 2021. [Online]. Available: https://www.khan.co.kr/national/incident/article/202103091200001

[13] S. Gatlan, "REvil ransomware affiliates arrested in Romania and Kuwait," BleepingComputer, Nov. 08, 2021. https://www.bleepingcomputer.com/news/security/revil-ransomware-affiliates-arrested-in-romania-and-kuwait/ (accessed Nov. 22, 2021).

[14] M.-A. Russon, "US fuel pipeline hackers 'didn't mean to create problems,'" BBC News, May 10, 2021. Accessed: May 24, 2021. [Online]. Available: https://www.bbc.com/news/business-57050690

[15] Herjavec Group Threat Team, "State of Ransomware 2021 Q1-Q2," Herjavec Group, Jul. 2021. Accessed: Oct. 12, 2021. [Online]. Available: https://herjavecgroup.sharepoint.com/sites/ThreatTeam/Shared%20Documents/Resources/Example%20output/Herjavec-Group-State-of-Ransomware-Report-1H-2021.pdf

[16] Threat & Vulnerability Management Team, "BlackMatter: Adversary Profile."

[17] Microsoft Threat Intelligence Center, "Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021 - Microsoft Security Blog," Microsoft Security Blog, Nov. 16, 2021. https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/ (accessed Nov. 22, 2021).

[18] B. Toulas, "Moses Staff hackers wreak havoc on Israeli orgs with ransomless encryptions," BleepingComputer. Accessed: Nov. 22, 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/moses-staff-hackers-wreak-havoc-on-israeli-orgs-with-ransomless-encryptions/

[19] "Benny Gantz's cleaner charged with Black Shadow spying bid." https://www.aljazeera.com/news/2021/11/18/benny-gantz-cleaner-charged-with-black-shadow-spying-bid (accessed Nov. 23, 2021).

[20] "BlackShadow hackers breach Israeli hosting firm and extort customers," BleepingComputer. https://www.bleepingcomputer.com/news/security/blackshadow-hackers-breach-israeli-hosting-firm-and-extort-customers/ (accessed Nov. 23, 2021).

[21] "Israel charges Defense Minister's house cleaner with leaking data to Iranian hackers," The Record by Recorded Future, Nov. 19, 2021. https://therecord.media/israel-charges-defense-ministers-house-cleaner-with-leaking-data-to-iranian-hackers/ (accessed Nov. 23, 2021).

[22] "Chinese State-Sponsored Cyber Operations: Observed TTPs | CISA." https://us-cert.cisa.gov/ncas/alerts/aa21-200b (accessed Nov. 23, 2021).

[23] "Potential for China Cyber Response to Heightened U.S.–China Tensions | CISA." https://us-cert.cisa.gov/ncas/alerts/aa20-275a (accessed Nov. 23, 2021).

[24] "Top 10 Routinely Exploited Vulnerabilities | CISA." https://us-cert.cisa.gov/ncas/alerts/aa20-133a (accessed Nov. 23, 2021).

[25] N. S. Agency, "Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities," National Security Agency, Oct. 2020. Accessed: Oct. 23, 2020. [Online]. Available: https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF

[26] "Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities | Volexity." https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/ (accessed Nov. 23, 2021).

[27] "HAFNIUM targeting Exchange Servers with 0-day exploits," Microsoft Security Blog, Mar. 02, 2021. https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ (accessed Nov. 23, 2021).

[28] "Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling," Recorded Future, Jul. 08, 2021. https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/ (accessed Nov. 23, 2021).

[29] M. Tartare, "Winnti Group targeting universities in Hong Kong," Jan. 31, 2020. https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/ (accessed Feb. 03, 2020).

[30] PTSecurity, "ShadowPad: new activity from the Winnti group," PTSecurity, Sep. 2020. Accessed: Oct. 08, 2020. [Online]. Available: https://www.ptsecurity.com/upload/corporate/ww-en/pt-esc/winnti-2020-eng.pdf

[31] Mandiant, "'Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests," Mandiant, Jul. 2020. Accessed: Jul. 30, 2020. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf

[32] Mandiant Threat Intelligence, "Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity," Adversary Profile, Apr. 2021.

[33] "Russia, Belarus agree to integrate gas, financial markets," AP NEWS, Nov. 04, 2021. https://apnews.com/article/business-russia-vladimir-putin-moscow-belarus-93a79aff811d535bc9e9d5d0a3dc5969 (accessed Nov. 23, 2021).

[34] "UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests | Mandiant." https://www.mandiant.com/resources/unc1151-linked-to-belarus-government (accessed Nov. 23, 2021).

[35] "Operation Secondary Infektion Targets Pfizer Vaccine," Recorded Future, Oct. 20, 2021. https://www.recordedfuture.com/seconday-infektion-targets-pfizer-vaccine/ (accessed Nov. 17, 2021).

[36] "Operation Secondary Infektion Impersonates Swedish Riksdag, Targets European Audiences," p. 9.

[37] C. Osborne, "Chief exec of cybersecurity Group-IB arrested on treason charge," ZDNet. https://www.zdnet.com/article/chief-exec-of-cybersecurity-group-ib-arrested-on-treason-charge/ (accessed Nov. 19, 2021).

[38] "Group-IB founder arrested in Moscow on state treason charges," The Record by Recorded Future, Sep. 29, 2021. https://therecord.media/group-ib-founder-arrested-in-moscow-on-state-treason-charges/ (accessed Nov. 19, 2021).

[39] "Group-IB's statement on the events of Sep. 28 at the company's office in Moscow," Group-IB. https://www.group-ib.com/media/official-statement-group-ib/ (accessed Nov. 19, 2021).

[40] "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report | Reuters." https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX (accessed Nov. 23, 2021).

[41] GReAT, "Operation AppleJeus Sequel," Jan. 08, 2020. https://securelist.com/operation-applejeus-sequel/95596/ (accessed Jan. 13, 2020).

[42] B. Marczak, J. Scott-Railton, S. McKune, B. A. Razzak, and R. Deibert, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Sep. 18, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ (accessed Nov. 21, 2019).

[43] S. Kirchgaessner, "Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests," The Guardian, Jul. 18, 2021. Accessed: Nov. 17, 2021. [Online]. Available: https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus

References

[44] "Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince' | Technology | The Guardian." https://web.archive.org/web/20200229191904/https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince (accessed Nov. 17, 2021).

[45] "From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits," The Citizen Lab, Aug. 24, 2021. https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/ (accessed Aug. 24, 2021).

[46] M. Kenyon, "Citizen Lab Response to the U. N. Working Group on the Use of Mercenaries," Citizen Lab, University of Toronto, Feb. 2021. Accessed: Nov. 17, 2021. [Online]. Available: https://citizenlab.ca/2021/02/citizen-lab-response-to-the-u-n-working-group-on-the-use-of-mercenaries/

[47] "Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware," University of Toronto, Citizen Lab Research Report No. 146, Nov. 2021. Accessed: Nov. 17, 2021. [Online]. Available: https://citizenlab.ca/2021/11/palestinian-human-rights-