SecurityScorecard

STRIKE

Cyber Risk Intelligence (CRI) Monthly Report

PALADIN COMMUNICATIONS

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th St
Suite 15-001
New York, NY 10017
1.800.682.1707

September 2022

This report presents the information and findings of SecurityScorecard’s Threat Research, Intelligence, Knowledge and Engagement (STRIKE) Team and is intended solely for informational purposes. For the avoidance of doubt, and notwithstanding anything to the contrary in this report or in any agreement between you and SecurityScorecard, SecurityScorecard disclaims all representations and warranties, express, implied, statutory and otherwise, with respect to this report and the information and findings contained herein, all of which are provided “as is” and without warranty. SecurityScorecard expressly disclaims the implied warranties of title, merchantability, fitness for a particular purpose and non-infringement.

EXECUTIVE SUMMARY

RISK EXPOSURE DASHBOARD

Leaked Credentials	Impostor Domains	Hacker Chatter	APT Reconnaissance
MEDIUM	MEDIUM	LOW	HIGH

Paladin Communication's (Paladin) cyber risk exposure for September 2022 is rated at medium-high risk. The main factor behind this rating is the discovery of a session between Paladin's webserver and an IP address associated with Russian state-sponsored cyber group APT28.   Due to this connection, Paladin should be on a heightened alert for a potential attack from APT28, possibly in retaliation for Western sanctions imposed on Russia. Other factors affecting this risk rating include the discovery of clear text passwords associated with a high ranking Paladin employee and several impostor domains. Immediate efforts should be directed towards monitoring for further APT28 activity, resetting a password exposed online, blocking identified imposter domains, and considering assigning unique passwords to Paladin's residential routers.

LEAKED CREDENTIALS

STRIKE queried its sources for Paladin-related leaked credentials and discovered the corporate email address of Paladin's current Chief Governance and Legal Officer, John Smith, were exposed as part of the LinkedIn data breach in 2012, and again in the People Data Labs breach in 2019. In addition to LinkedIn and Facebook credentials, the breach also exposed his phone number and clear text passwords. Hackers with malicious intent can use this information to gain access to social media accounts, or to enable social engineering and phishing attacks.

Key Takeaway:

A detailed list of the aforementioned leaked credentials and personal information will be provided out of band by your account manager. In the meantime, Paladin should force a reset of Mr. Smith's corporate password and audit logs for any authorized access. Paladin should also consider advising employees not to sign up for social media accounts using their corporate email addresses.

IMPOSTER DOMAINS

STRIKE detected the registration of the following four domains impersonating Paladin Communication's legitimate domain. These domains will likely be used to support phishing and social engineering attacks on Paladin's employees and customers.

DOMAIN	IP	REGISTRANT	CREATED DATE/TIME
pa1adinc0mmnunicat10ns[.]mobi1	69.43.91[.]24N	NameCheap	September 2nd, 16:34 UTC
pa1adinc0mmnunicat10ns[.]mobi1	69.55.52[.]25	NameCheap	September 2nd, 16:34 UTC
palad1nc0mmunicat10ns[.]biz	169.3.4[.]108W	WildWestDomains	September 15th, 10:29 UTC
paladincommunications[.]xyz	169.4.5[.]45	GoDaddy	September 23rd, 22:34 UTC

The STRIKE Team ran searches for the aforementioned IPs and Domains in our intelligence holdings. IPs 169.43.91[.]24 and 169.55.52[.]25 have a long history of hosting domains associated with phishing and campaigns. The IPs are hosted by Stark Industries Inc., a "bulletproof" hosting provider that doesn't require documentation and accepts payment in digital currency, making it popular amongst threat actors.

Key Takeaway:

Paladin should block access to these domains in its firewall so that if they are used in phishing attacks, users will not be able to access them if they click the malicious link. Paladin should also consider registering its legitimate domain with as many TLDs as possible so that they are not available to threat actors.

STRIKE has escalated these domains to Google's phishing protection team for further analysis and blocking.

HACKER CHATTER

Ransomware Group Mentions

STRIKE did not observe any Paladin-related mentions on websites or forums controlled by Ransomware groups. Nonetheless, ransomware attacks were detected in the Telecommunications industry this month. SecurityScorecard observed ransomware and data extortion attacks on smaller telcos. According to SecurityScorecard's Ransomware/Data Extortion breach data, multiple Ransomware groups have been active in these activities, such as Lockbit, Conti, Hive, Everest, Ragnar Locker, Everest, AvosLocker, and Lorenz, which all claimed to have successfully breached Financial Services Industry (FSI) companies.

Key Takeaway:

- Given the prevalence and high potential impact of Ransomware and Data Extortion attacks, SecurityScorecard recommends that organizations implement the following controls:
- Have a robust backup program that captures data at adequate time periods and is stored out of band, where there is no chance of it being encrypted by threat actors. Simulate restoring to backup data so when the time comes, this process is well understood and efficiently implemented.
- Ensure sensitive data is encrypted with the appropriate level of security according to regulations and laws. Non-nation-state hackers typically do not have the resources or skill to decrypt data, rendering it useless.
- Keep operating systems, software, and applications current and up-to-date.
- Ensure antivirus and anti-malware solutions are set to automatically update, and then run regular scans.
- Identify and secure network devices running risky services such as Remote Desktop Protocol (RDP) and Virtual Network Computing (VNC). We recommend deploying a solution like SecurityScorecard's Attack Surface Intelligence (ASI) product to proactively identify risky and vulnerable services, protocols, and devices on your network.

Dark Web Mentions

STRIKE observed a mention of Paladin on the hacking forum exploitsrus[.]com on September 4th. Forum user @Anazon posted that they had successfully hacked his neighbor's Paladin Internet Service router by entering the default username and password (admin/admin). @Anazon indicated that once they accessed the router, they throttled down the bandwidth, which would "infuriate his neighbor." He also changed the password so his neighbor could not access the router to re-configure it.

Key Takeaway:

Paladin should consider deploying a more secure password policy for its routers and network products. Routers and other devices should each have their unique passwords. If this is not possible, customers should be strongly advised to reset the default password to something more secure.

INDICATORS OF APT RECONNAISSANCE

STRIKE detected several connections between infrastructure associated with APT28 and Paladin. On September 22nd at 09:23:38, a connection was made from IP address 152.168.9[.]2, known to be used by APT28, to Paladin's main website www.paladincommunications.com. The connection lasted 28 minutes. This activity could indicate that APT28 was conducting reconnaissance for a future campaign against the Paladin.

Key Takeaway:

Given this connection, Paladin should be on a heightened alert for a potential attack from APT28. APT28's main modus operandi is intelligence collection, not disruption. However, it has been involved in both. Given the sanctions currently in place against Russia, APT28 may have been given orders to strike back at Western telecommunications firms in retaliation. STRIKE advises Paladin to review its web server logs for connections with this IP address to identify the exact pages that were visited. Monitoring logs for this IP is favorable to blocking the IP address, as the former provides intelligence, whereas the latter simply forces APT28 to use a different IP address—one that may not be known to be associated with them—thus losing visibility into the potential campaign.

The following threat actor profile provides more information on APT28's Tactics, Techniques, and Procedures:

Threat Actor Profile - APT28

Aliases: Grizzly Steppe, Swallowtail, Sednit, SIG40, ATK5, TG-4127, TsarTeam, Group-4127, apt_sofacy, IRON TWILIGHT, PawnStorm, G0007, Pawn Storm, Tsar Team, Group 74, APT 28, APT28, Fancy Bear, STRONTIUM, SNAKEMACKEREL, TAG_0700

Origin: Russia

Description: APT28 is a cyber espionage group believed to have ties to the Russian government, specifically The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.

Targeted Countries: France, China, Turkey, United Kingdom, Georgia, Hungary, Kazakhstan, Japan, Jordan, Germany, Tajikistan, Ukraine, United States, Armenia, Mongolia, Afghanistan, Poland, Belgium, and Pakistan.

Targeted Entities: European Commission, Asia Pacific Economic Cooperation, NATO, OSCE, International Association of Athletics Federations, World Anti-Doping Agency

Targeted industries: Government, Military, Political, Sports Authoritative Bodies

Industry Insights:

https://www.handelsblatt.com/today/politics/election-risks-russia-linked-hackers-target-german-political-foundations/23569188.html?ticket=ST-2696734-GRHgtQukDIEXeSOwksXO-ap1

https://www.bbc.com/news/technology-37590375

https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/

https://www.eff.org/deeplinks/2015/08/new-spear-phishing-campaign-pretends-be-eff

https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/

https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/

https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/

https://www.lse.co.uk/AllNews.asp?code=kwdwehme&headline=Russian_Hackers_Suspected_In_Cyberattack_On_German_Parliament

https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected

https://en.wikipedia.org/wiki/Fancy_Bear

https://www.bbc.co.uk/news/technology-45257081

https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/

https://unit42.paloaltonetworks.com/unit42-let-ride-sofacy-groups-dealerschoice-attacks-continue/

https://www.accenture.com/t20181129T203820Z__w__/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf

https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/

https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/

https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/

https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government

https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/

https://www.dw.com/en/hackers-lurking-parliamentarians-told/a-19564630

https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/

https://researchcenter.paloaltonetworks.com/2016/06/unit42-new-sofacy-attacks-against-us-government-agency/

https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html

https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/

https://www.ibtimes.co.uk/russian-hackers-fancy-bear-likely-breached-olympic-drug-testing-agency-dnc-experts-say-1577508

https://aptnotes.malwareconfig.com/web/viewer.html?file=../APTnotes/2014/apt28.pdf

https://www.msn.com/en-nz/news/world/russian-hackers-accused-of-targeting-un-chemical-weapons-watchdog-mh17-files/ar-BBNV2ny

https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

https://attack.mitre.org/groups/G0007/

https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/

https://en.wikipedia.org/wiki/Sofacy_Group

https://securelist.com/a-slice-of-2017-sofacy-activity/83930/

https://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/

https://www.washingtonpost.com/technology/2019/02/20/microsoft-says-it-has-found-another-russian-operation-targeting-prominent-think-tanks/?utm_term=.870ff11468ae

https://www.cfr.org/interactive/cyber-operations/apt-28

https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/

https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

https://www.voanews.com/a/iaaf-hack-fancy-bears/3793874.html

https://www2.fireeye.com/rs/848-DID-242/images/wp-mandiant-matryoshka-mining.pdf

https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware

https://www.volkskrant.nl/cultuur-media/russen-faalden-bij-hackpogingen-ambtenaren-op-nederlandse-ministeries~b77ff391/

https://marcoramilli.com/2019/12/05/apt28-attacks-evolution/

https://www.reuters.com/article/us-sweden-doping/swedish-sports-body-says-anti-doping-unit-hit-by-hacking-attack-idUSKCN1IG2GN

https://www.accenture.com/t20190213T141124Z__w__/us-en/_acnmedia/PDF-94/Accenture-SNAKEMACKEREL-Threat-Campaign-Likely-Targeting-NATO-Members-Defense-and-Military-Outlets.pdf https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/

https://www.apnews.com/4d174e45ef5843a0ba82e804f080988f

https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf

https://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/

SecurityScorecard

STRIKE

ABOUT STRIKE TEAM

CRI is delivered by the STRIKE Team, SecurityScorecard's elite team of cyber security experts with over 100 years of collective experience in cyber security investigations and research. STRIKE Team members come for varying backgrounds, including experience with intelligence services, special operations units, and Fortune 50 cyber threat intelligence teams.

ABOUT SECURITYSCORECARD

SecurityScorecard offers a 360-degree approach to security prevention and response. For more information, request a demo. SecurityScorecard's threat research and intelligence could be the competitive advantage organizations need to stay ahead of today's fast-moving threat actors.

For more custom insights on a regular basis through our team's 100+ years of combined threat research and investigation experience, or more details on these findings and the other keywords that were provided, please **speak to an expert** for a discussion of our Cyber Risk Intelligence (CRI) offering. If you have already suffered a breach, SecurityScorecard's **Digital Forensics Solutions** can empower your post-breach actions.