A Decade Of 'Bad Magic' In Cyber Espionage

Uploaded on 2023-07-05 in FREE TO VIEW (https://www.cybersecurityintelligence.com/blog/category/free-to-view-25.html)

New findings about a hacker group called 'Bad Magic,' which is linked to cyber attacks targeting companies in the Russia-Ukrainian conflict area, reveal that it may have been around for much longer than previously thought, according to leading cyber security firm Kaspersky (https://www.cybersecurityintelligence.com/kaspersky-lab-1402.html).

"In March 2023, we uncovered a previously unknown APT campaign in the region of the Russo-Ukrainian conflict that involved the use of PowerMagic and CommonMagic implants. However, at the time it was not clear which threat actor was behind the attack.

"Since the release of our report about CommonMagic, we have been looking for additional clues that would allow us to learn more about this actor. As we expected, we have been able to gain a deeper insight into the Bad Magic story," says Kaspersky. "While looking for implants bearing similarities with PowerMagic and CommonMagic, we identified a cluster of even more sophisticated malicious activities originating from the same threat actor.

"What was most interesting about it is that its victims were located not only in the Donetsk, Lugansk and Crimea regions, but also in central and western Ukraine. Targets included individuals, as well as diplomatic and research organisations."

The campaign is characterised by the use of a novel modular framework codenamed CloudWizard, which features capabilities to take screenshots, record microphone, log keystrokes, grab passwords, and harvest Gmail inboxes.

Bad Magic was first report in March 2023, detailing the group's use of a backdoor called PowerMagic (aka DBoxShell or GraphShell) and a modular framework dubbed CommonMagic in attacks targeting Russian-occupied territories of Ukraine.

Kaspersky (https://www.kaspersky.co.uk/about/press-releases/2023_kaspersky-researchers-uncover-an-ongoing-apt-campaign-targeting-organizations-located-in-the-russo-ukrainian-conflict-area): You Tube (http://www.youtube.com/watch?v=H2UfV3LNso8): Red Packet Security (http://www.redpacketsecurity.com/bad-magic-s-extended-reign-in-cyber-espionage-goes-back-over-a-decade/): Secure List (http://securelist.com/cloudwizard-apt/109722/): Hacker News (http://thehackernews.com/2023/05/bad-magics-extended-reign-in-cyber.html): CPO Magazine (http://www.cpomagazine.com/cyber-security/malware-used-for-cyber-espionage-since-2004-shut-down-in-us-after-years-long-fbi-operation/):

You Might Also Read:

Shuckworm Intensifies Cyber Attacks On Ukraine (https://www.cybersecurityintelligence.com/blog/shuckworm-intensifies-cyber-attacks-on-ukraine-7026.html):

« The Limitations of AI (https://www.cybersecurityintelligence.com/blog/the-limitations-of-ai-6988.html)

A New Approach To Cyber Security Helps Resist Extortion » (https://www.cybersecurityintelligence.com/blog/a-new-approach-to-cyber-security-helps-resist-extortion-6993.html)

(/cybersecurityjobs.php)

Sign Up: Cyber Security Intelligence Newsletter (https://cybersecurityintelligence.us3.list-manage.com/subscribe?u=a7a85ac110ceb74440637343f&id=eae4032b75)

Directory of Suppliers

MIRACL (https://www.cybersecurityintelligence.com/miracl.html)
MIRACL provides the world's only single step Multi-Factor Authentication (MFA) which can replace passwords on 100% of mobiles, desktops or even Smart TVs.
(https://www.cybersecurityintelligence.com/miracl.html)

NordLayer (https://www.cybersecurityintelligence.com/nordlayer.html)
NordLayer is an adaptive network access security solution for modern businesses — from the world's most trusted cybersecurity brand, Nord Security.
(https://www.cybersecurityintelligence.com/nordlayer.html)

ManageEngine (https://www.cybersecurityintelligence.com/manageengine.html)
As the IT management division of Zoho Corporation, ManageEngine prioritizes flexible solutions that work for all businesses, regardless of size or budget.
(https://www.cybersecurityintelligence.com/manageengine.html)

Authentic8 (https://www.cybersecurityintelligence.com/authentic8.html)
Authentic8 transforms how organizations secure and control the use of the web with Silo, its patented cloud browser.
(https://www.cybersecurityintelligence.com/authentic8.html)

LockLizard (https://www.cybersecurityintelligence.com/locklizard.html)
Locklizard provides PDF DRM software that protects PDF documents from unauthorized access and misuse. Share and sell documents securely - prevent document leakage, sharing and piracy.
(https://www.cybersecurityintelligence.com/locklizard.html)

Information Security Media Group (ISMG) (https://www.cybersecurityintelligence.com/information-security-media-group-ismg.html)
Information Security Media Group is the world's largest media organization devoted solely to information security and risk management.
(https://www.cybersecurityintelligence.com/information-security-media-group-ismg.html)

Covenco (https://www.cybersecurityintelligence.com/covenco.html)
Covenco is a data management and IT infrastructure specialist. Working with customers to transform their IT environments, with data protection and security at the forefront of everything we do.
(https://www.cybersecurityintelligence.com/covenco.html)

Conference-Service.com (https://www.cybersecurityintelligence.com/conference-servicecom.html)
Conference-Service.com provides a categorised calendar of conferences and events which includes Information Security.
(https://www.cybersecurityintelligence.com/conference-servicecom.html)

PeCERT (https://www.cybersecurityintelligence.com/pecert.html)
PeCERT is the national Computer Emergency Response Team for Peru.
(https://www.cybersecurityintelligence.com/pecert.html)

Inogesis (https://www.cybersecurityintelligence.com/inogesis.html)
(https://www.cybersecurityintelligence.com/inogesis.html)

Redborder (https://www.cybersecurityintelligence.com/redborder.html)

Redborder is an Open Source network visibility, data analytics, and cybersecurity Big Data solution that is scalable up to the needs of enterprise networks and service providers.

(https://www.cybersecurityintelligence.com/redborder.html)

XM Cyber (https://www.cybersecurityintelligence.com/xm-cyber.html)

XM Cyber is a leading hybrid cloud security company that's changing the way innovative organizations approach cyber risk.

(https://www.cybersecurityintelligence.com/xm-cyber.html)

Innovent Recycling (https://www.cybersecurityintelligence.com/innovent-recycling.html)

Innovent Recycling provides a secure IT recycling & data destruction service to all types of organizations across the UK.

(https://www.cybersecurityintelligence.com/innovent-recycling.html)

VIBE Cybersecurity International (https://www.cybersecurityintelligence.com/vibe-cybersecurity-international.html)

VIBE's certificate-less authenticated encryption enables scalable, flexible key exchange, and other advanced cryptographic functions using identity-based elliptic curve cryptosystems (ECC).

(https://www.cybersecurityintelligence.com/vibe-cybersecurity-international.html)

Global Cyber Security Capacity Centre (GCSCC) - Oxford University (https://www.cybersecurityintelligence.com/global-cyber-security-capacity-centre-gcscc---oxford-university.html)

GCSCC's work is focused on developing a framework for understanding what works, what doesn't work and why – across all areas of cybersecurity capacity.

(https://www.cybersecurityintelligence.com/global-cyber-security-capacity-centre-gcscc---oxford-university.html)

Swedish Incubators & Science Parks (SISP) (https://www.cybersecurityintelligence.com/swedish-incubators-and-science-parks-sisp.html)

Swedish Incubators & Science Parks (SISP) is the Swedish industry association for Swedish incubators and science parks.

(https://www.cybersecurityintelligence.com/swedish-incubators-and-science-parks-sisp.html)

Information & Communications Technology Association of Jordan (int@j) (https://www.cybersecurityintelligence.com/information-and-communications-technology-association-of-jordan-intj.html)

The Information & Communications Technology Association of Jordan is a membership based ICT and IT Enabled Services (ITES) industry advocacy, support and networking association.

(https://www.cybersecurityintelligence.com/information-and-communications-technology-association-of-jordan-intj.html)

Lancera (https://www.cybersecurityintelligence.com/lancera.html)

Lancera provides growth accelerating Software Development, Web Presence and Cybersecurity Solutions with a focus on customer happiness.

(https://www.cybersecurityintelligence.com/lancera.html)

Celera Networks (https://www.cybersecurityintelligence.com/celera-networks.html)

Celera Networks is a managed services provider specializing in cybersecurity, cloud and managed IT services.

(https://www.cybersecurityintelligence.com/celera-networks.html)

Aiden Technologies (https://www.cybersecurityintelligence.com/aiden-technologies.html)

Aiden simplifies your IT process, giving you peace of mind and security by ensuring your computers get exactly the software they need and nothing else.

(https://www.cybersecurityintelligence.com/aiden-technologies.html)

Verastel (https://www.cybersecurityintelligence.com/verastel.html)

Specializing in the niche space of proactive cyber-defense, and adaptive resilience, team Verastel is bolstering enterprise digital security like never before.

(https://www.cybersecurityintelligence.com/verastel.html)

BUSINESS
Energy (https://www.cybersecurityintelligence.com/blog/category/business-production-energy-5.html)
Manufacturing (https://www.cybersecurityintelligence.com/blog/category/business-production-manufacturing-3.html)
Utilities (https://www.cybersecurityintelligence.com/blog/category/business-production-utilities-2.html)
Consulting (https://www.cybersecurityintelligence.com/blog/category/business-services-consulting-9.html)
Financial (https://www.cybersecurityintelligence.com/blog/category/business-services-financial-4.html)
Health & Welfare (https://www.cybersecurityintelligence.com/blog/category/business-services-health-and-welfare-7.html)
IT & Communications (https://www.cybersecurityintelligence.com/blog/category/business-services-it-and-communications-8.html)
Law (https://www.cybersecurityintelligence.com/blog/category/business-services-law-6.html)
Transport & Travel (https://www.cybersecurityintelligence.com/blog/category/business-services-transport-and-travel-33.html)
GOVERNMENT
Defence (https://www.cybersecurityintelligence.com/blog/category/government-defence-11.html)
Law Enforcement (https://www.cybersecurityintelligence.com/blog/category/government-law-enforcement-14.html)
Local (https://www.cybersecurityintelligence.com/blog/category/government-local-13.html)
National (https://www.cybersecurityintelligence.com/blog/category/government-national-12.html)
TECHNOLOGY
Developments (https://www.cybersecurityintelligence.com/blog/category/technology--developments-15.html)
Hackers (https://www.cybersecurityintelligence.com/blog/category/technology-hackers-17.html)
Resilience (https://www.cybersecurityintelligence.com/blog/category/technology--resilience-18.html)
5G Networks (https://www.cybersecurityintelligence.com/blog/category/technology-key-areas-5g-networks-35.html)
Artificial Intelligence (https://www.cybersecurityintelligence.com/blog/category/technology-key-areas-artificial-intelligence-36.html)
Blockchain (https://www.cybersecurityintelligence.com/blog/category/technology-key-areas-blockchain-37.html)
Internet Of Things (https://www.cybersecurityintelligence.com/blog/category/technology-key-areas-internet-of-things-38.html)
Social Media (https://www.cybersecurityintelligence.com/blog/category/technology-social-media-16.html)
INTELLIGENCE
Europe (https://www.cybersecurityintelligence.com/blog/category/intelligence-europe-29.html)
International (https://www.cybersecurityintelligence.com/blog/category/intelligence-international-30.html)
US (https://www.cybersecurityintelligence.com/blog/category/intelligence-u-28.html)
China (https://www.cybersecurityintelligence.com/blog/category/intelligence-hot-spots-china-24.html)
Iran (https://www.cybersecurityintelligence.com/blog/category/intelligence-hot-spots-iran-40.html)
North Korea (https://www.cybersecurityintelligence.com/blog/category/intelligence-hot-spots-north-korea-41.html)
Russia (https://www.cybersecurityintelligence.com/blog/category/intelligence-hot-spots-russia-42.html)
DIRECTORY
Browse Categories (https://www.cybersecurityintelligence.com/browse_categories.php)
Browse Locations (https://www.cybersecurityintelligence.com/browse_locations.php)
Advanced Search (https://www.cybersecurityintelligence.com/search.php)
ABOUT US
Contact (https://www.cybersecurityintelligence.com/contact.php)
Who We Are (https://www.cybersecurityintelligence.com/pages/who-we-are.html)
Commercial Terms (https://www.cybersecurityintelligence.com/pages/commercial-terms.html)
Register / Subscribe (https://www.cybersecurityintelligence.com/members/user_account_add.php)
Legal (https://www.cybersecurityintelligence.com/pages/legal.html)