

NETENRICH

I KNOWLEDGE NOW:

EVERYTHING YOU NEED TO KNOW ABOUT CYBER THREATS – IN MINUTES, FREE

Even with enough cybersecurity experts to go around, you never have time to stay on top of all the news. Until now. Or should we say, until KNOW?

The Knowledge NOW (KNOW) Threat Intelligence app from Netenrich puts time on your side, starting with placing the days' top stories in your inbox every day.

KNOW makes it easy to dig deep into breaking news, evolving trends, and the threats and IOCs that matter to you.

Get all the news, perspective, and intelligence you need in one place — FREE — to answer pressing SecOps questions in minutes versus hours, days, and weeks.

What happened?

Start your day in the KNOW with Netenrich's daily newsletter. *KNOW TODAY* places the day's top stories in your inbox so you never miss a thing, and don't need to spend hours checking other sites just to stay informed.

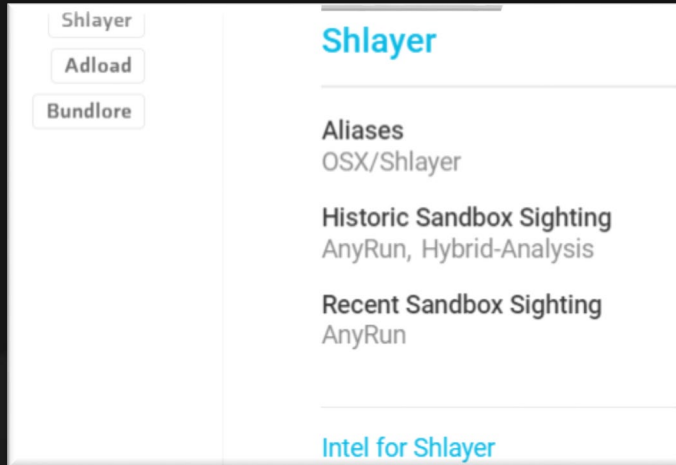
When something sparks your interest, log into the KNOW intelligence portal for the **who, where, why, and how.**



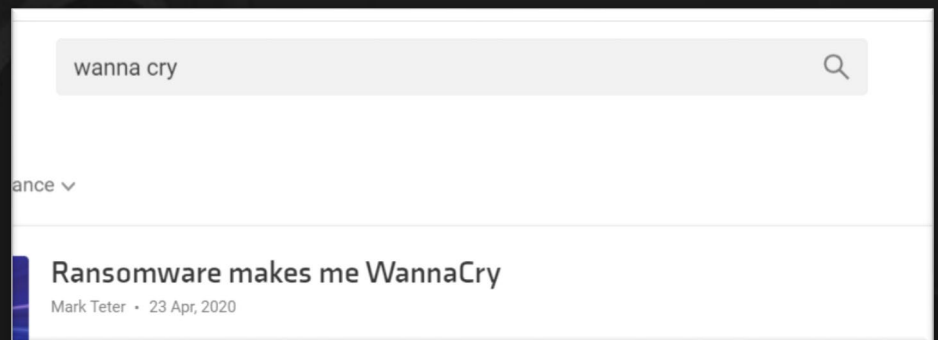
What are the experts saying about it?

Log into KNOW to search today's breaking news and IoCs you find on your own. Netenrich uses advanced AI to scan millions of web pages, blog feeds, publications, authors, posts, social media feeds, and OSINT feeds every day. Intelligent filtering and complex algorithms correlate news, trends, analysis, and historical insight to deliver rich, actionable context. Analyst-vetted "tags" and "related topics" help you track exploits, vulnerabilities, and attacks relevant to your unique threat landscape.

What should we be following?



The context provided by KNOW makes it easy to find news outlets, experts, and related trends to follow. Use features like "Saved Searches," "Related Trends," and "Threats You Follow" to make sure you always KNOW first when something happens.



What changed since yesterday?

Long after zero-day attacks make headlines, adversaries find new ways to use them. KNOW makes it easy to track the latest developments on attacks, exploits, IoCs, and other topics of interest — without having to check multiple sources, so you never miss a beat again!

What does it mean to us?

Your WordPress installation has put you at risk to brute force and denial of service attacks.

AFFECTED ENTITY
https://www.abcxyz.com/contact.php

Threat Impact
High

Attackers can hijack your brand trust to infect your customers or take complete control of your site.

AFFECTED ENTITY
https://www.abcxyz.com/contact/thank-you/?http_zip

Reflected cross-site scripting (XSS) vulnerability was discovered in eighthealth.com, which will allow attackers to insert HTML and JavaScript code to deface the website and steal sensitive information. XSS technique can be leveraged to send a malicious script to an unsuspecting user.

The end user's browser has no way to know that the script should not be trusted and will execute the script. The malicious script can access any cookies, session tokens, or other sensitive information stored by the browser and used within that site.

An attacker can send a malicious link via e-mail, messenger, etc. As the victim trusts the brand domain eighthealth.com, will click the link and can be redirected to a site hosting malware or exploit.

Steps to reproduce

Open the following URL in browser:
https://www.abcxyz.com/contact/thank-you/?http_zip%27%3C%3Cimg%3Dsrc%3Dx%3Dx%3D%3Dalert%27%3D%3D%3E

An alert box with "XSS" would appear. This means that an attacker has full control of the scripts, that are executed in the victim browser context. The parameter http_zip is vulnerable to such attacks.

Reasons you should be worried

ServiceDesk Plus vulnerability could give attackers full access to IT support systems
https://www.socpanda.com/2019/08/08/service-desk-plus-vulnerability-could-give-attackers-full-access-to-it-support-systems

WE RECOMMEND

User input needs to be encoded in the HTTP header and developer can implement filters which will eliminate any scripting tags. In some cases, "X-SS-Protection" header can prevent some kind of XSS. Cross-site-scripting attacks as it's an add-on to the browsers to sanitize HTML responses.

WordPress XML-RPC with your website ricked to perform force attack. The is of the RPC which ng a POST request

methodName>

ance can be used to kernal service. ke this:

ame>

string></value> wordpress-site</string>

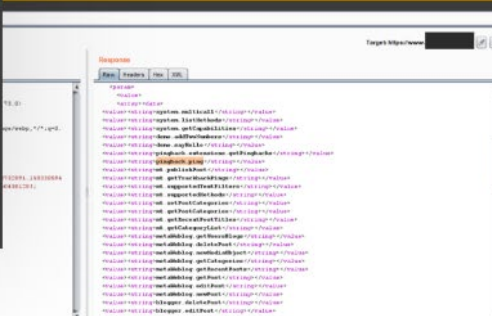
The above request can be repeated to http://external-website as many times one wants; thus your wordpress could become victim of a large botnet of attacking websites. Not just that, using the method 'system.multicall' one could execute multiple method in a single request. Which would mean one can brute force 1000+ user names/passwords combination in just one request.

Similarly using the method 'wp.getUsersBlogs' one could try to brute force username and password till the response is positive.

Reasons you should be worried

More Than 162,000 WordPress Sites Used for Distributed Denial of Service Attack
<https://blog.sucuri.net/2014/03/more-than-162000-wordpress-sites-used-for-distributed-denial-of-service-attack.html>

being used, it should be disabled and removed completely to avoid any should at the very least be blocked from external access



Report generated on 05 Mar, 2020 | Abc Xyz Netenrich, Inc.

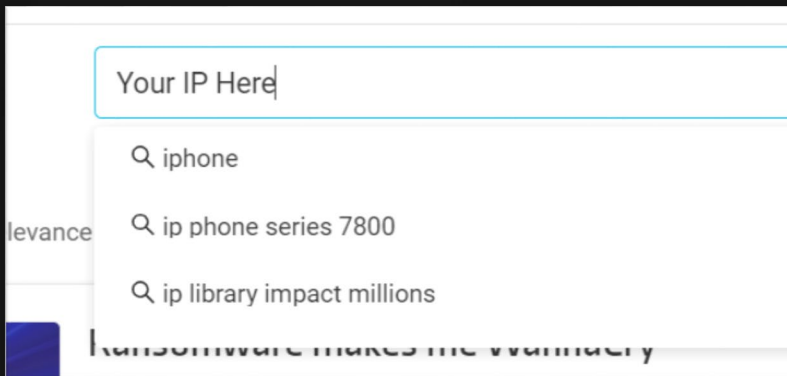
At the end of the day, what you really want to know is whether and how you should act on threats and trends. Bringing news and intelligence together in one place helps answer the ultimate SecOps questions: Why did this attack succeed? Could it happen to us? How do we act first to stop it?

KNOW integrates with Netenrich's Attack Surface Intelligence (ASI) solution to provide complete Resolution Intelligence for managing your company's unique threat landscape. ASI shows where your brand is exposed to digital risk on the public Internet and leverages KNOW to fast-track analysis, prioritization, and mitigation strategies.

How do we KNOW if it's good or bad?

KNOW goes beyond one-way threat intelligence to save you time researching bad IPs, IoCs, and other data from your Attack Surface Intelligence solutions.

BRING YOUR OWN THREATS!



What else do we need to KNOW?

Timely data and rich context help you act and become more proactive over time. Use intelligence from KNOW to optimize and improve:

- Incident response
- Vulnerability and external risk management
- Update and patch prioritization
- Alert fatigue
- Reporting to CISOs, CIOs, business line managers, and other stakeholders

Visit
know.netenrich.com to
stay in the KNOW.

IT'S FREE!