DomainTools

LuJam CYBER

NOD CASE STUDY

LuJam Leverages Farsight Security's Newly Observed Domains (NOD) Solution to Address Zero-Day Attacks

The Customer

LuJam Cyber was founded in 2014 when its CEO Tim Moran realized that small and mid-sized businesses need similar levels of cyber security enjoyed by major enterprises, but delivered in a way that was easy for a business owner or manager to use, without having to be an IT specialist. Four years and extensive trials later, LuJam launched its Cyber Protection Service. The sub- scription service offers a jargon-free customer experience that gives visibility of all the devices connected to a network, while protecting it 24/7 against the latest cyber threats. In November 2018, LuJam was one of six start-ups invited to join the prestigious U.K. Cyber Accelerator programme run by the National Cyber Security Centre (NCSC) of the Government Communications Headquarters (GCHQ) offers a range of data solutions under the NOD service that present subscribers with real-time actionable insights on new domain names.

LuJam's Focus

LuJam provides enterprise security to small- and medi- um-size businesses in the United Kingdom, including law firms, real estate companies, and startups. These businesses consist of 1-20 users with approximately 30% home workers and no one dedicated to IT support. For the majority of their customers, normal security standards consist of firewalls and anti-virus tools only.

The Challenge

Keeping Pace with Cyberattacks

Armed only with traditional cyber defenses, LuJam customers struggle to keep up with the quantity and sophistication of cyberattacks. LuJam's Cyber Protection Service places sensors inside the customer's network to monitor, detect and protect against ransomware, malware, phishing and zero-day attacks. These sensors collect information on customer devices (i.e., what sites they visit), pairing a device to a site. For example, they may observe a device visiting certain sites outside their usual behavior and trend patterns.

"It is usually catastrophic when a customer is hit by a cyber-attack. It causes them to lose money—thousands of pounds of damage."

Closing the Gap

The biggest gap the LuJam team needed to close was zero-day attacks. Zero-day attacks occur when a software/hardware vulnerability is exploited and attackers release malware before a developer has an opportunity to create a fix.

Running 60+ customer networks, LuJam needed to bring in enterprise threat intelligence. LuJam initially purchased blacklists, yet these static indicators quickly became out-of-date and not effective against zero-day attacks. Bad actors would create, use, and throw away suspicious domains before they could be blocked.

The Solution

Leveraging Farsight Security's Newly Observed Domains (NOD) solution, LuJam ingests numerous threat intelligence feeds every 5 minutes and analyzes what's changed over the past 24 hours. Using DNS Masq, LuJam then sends new domains to each of their customer networks. If a domain name appears in NOD, users are redirected to a blocker page and it's recorded.

"Once a domain goes live, we push it down to our cutomers within six minutes. The customers are exposed to zero-days under six minutes or less."

The Results

Since implementing NOD in January 2018, LuJam has blocked more zero-days than ever before.

"There is a gap between companies becoming aware of a security issue and distribution of that information to its users. NOD closes that gap."

Why DomainTools?

"While we had a good relationship with a number of threat intelligence vendors, none had anything like NOD. Within two hours of signing the contract, we had the NOD list setup and running in a half-day—and have kept it running since then. It was easy to get it up and running and the format is perfect for us.

NOD should be part of any cyber arsenal and we would recommend NOD to other organizations. It is providing huge value for us.

Andy Ben-Dyke
Chief Technology Officer

About NOD

Farsight's Newly Observed Domains (NOD) solution provides organizations with real-time actionable insights based on the newness of a domain. This enables them to protect their users from newly configured and used domains until those domains are better understood by the rest of the security industry such as spam filters and reputation providers—thereby materially improving their risk profile.

NOD leverages Farsight's real-time Passive DNS sensor array and cross-references that data with its industry-leading DNSDB™ historical Passive DNS database.

DomainTools

About DomainTools
DomainTools is the global leader for internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.

View our Farsight DNSDB page