ESET Discovers Corporate Secrets and Data on Recycled Company Routers

DUBAI, UNITED ARAB EMIRATES, April 24, 2023 /EINPresswire.com/ -- ESET, a global leader in digital security, today unveiled new research into corporate network devices that were disposed of and sold on the secondary market. After looking at configuration data from 16 distinct network devices, ESET found that over 56% – nine routers – contained sensitive company data.

Of the nine networks that had complete configuration data available:

- 22% contained customer data
- 33% exposed data allowing third-party connections to the network
- 44% had credentials for connecting to other networks as a trusted party
- 89% itemized connection details for specific applications
- 89% contained router-to-router authentication keys
- 100% contained one or more of IPsec or VPN credentials, or hashed root passwords
- 100% had sufficient data to reliably identify the former owner/operator

“The potential impact of our findings is extremely concerning and should be a wake-up call,” said Cameron Camp, the ESET security researcher who led the project. “We would expect medium-sized to enterprise companies to have a strict set of security initiatives to decommission devices, but we found the opposite. Organizations need to be much more aware of what remains on the devices they put out to pasture, since a majority of the devices we obtained from the secondary market contained a digital blueprint of the company involved, including, but not limited to, core networking information, application data, corporate credentials, and information about partners, vendors, and customers.”

Organizations often recycle aging tech through third-party companies that are charged with verifying the secure destruction or recycling of digital equipment and the disposal of the data contained therein. Whether an error by an e-waste company or the company’s own disposal

processes, a range of data was found on the routers, including:

- Third-party data: As we have seen in real-world cyberattacks, a breach of one company's network can proliferate to their customers, partners, and other businesses with whom they may have connections.

- Trusted parties: Trusted parties (which could be impersonated as a secondary attack vector) would accept certificates and cryptographic tokens found on these devices, allowing a very convincing adversary in the middle (AitM) attack with trusted credentials, capable of syphoning off corporate secrets, with victims unaware for extended periods.
- Customer data: In some cases, core routers point to internal and/or external information stores with specific information about their owners' customers, sometimes stored on premises, which can open customers up to potential security issues if an adversary is able to gain specific information about them.

- Specific applications: Complete maps of major application platforms used by specific organizations, both locally hosted and in the cloud, were scattered liberally throughout the configurations of these devices. These applications range from corporate email to trusted client tunnels for customers, physical building security such as specific vendors and topologies for proximity access cards and specific surveillance camera networks, and vendors, sales and customer platforms, to mention a few. Additionally, ESET researchers were able to determine over which ports and from which hosts those applications communicate, which ones they trust, and which ones they do not. Due to the granularity of the applications and the specific versions used in some cases, known vulnerabilities could be exploited across the network topology that an attacker would already have mapped.

- Extensive core routing information: From core network routes to BGP peering, OSPF, RIP and others, ESET found complete layouts of various organizations' inner workings, which would provide extensive network topology information for subsequent exploitation, were the devices to fall into the hands of an adversary. Recovered configurations also contained nearby and international locations of many remote offices and operators, including their relationship to the corporate office – more data that would be highly valuable to potential adversaries. IPsec tunneling can be used to connect trusted routers to each other, which can be a component of WAN router peering arrangements and the like.
- Trusted operators: The devices were loaded with potentially crackable or directly reusable corporate credentials – including administrator logins, VPN details, and cryptographic keys – that would allow bad actors to seamlessly become trusted entities and thus to gain access across the network.

"There are well-documented processes for proper decommissioning of hardware, and this research shows that many companies are not following them rigorously when preparing devices for the secondary hardware market," said Tony Anscombe, Chief Security Evangelist at ESET. "Exploiting a vulnerability or spearphishing for credentials is potentially hard work. But our

research shows that there is a much easier way to get your hands on this data, and more. We urge organizations involved in device disposal, data destruction, and reselling of devices to take a hard look at their processes and ensure they are in compliance with the latest NIST standards for media sanitization."

The routers in this research originated at organizations ranging from medium-sized businesses to global enterprises in a variety of industries (data centers, law firms, third-party tech providers, manufacturing and tech companies, creative firms, and software developers). As part of the discovery process, ESET, where possible, disclosed the findings to each identified organization – several of them household names – collaborating to ensure they were aware of the details potentially compromised by others in the chain of custody of the devices. Some of the organizations with compromised information were shockingly unresponsive to ESET's repeated attempts to connect, while others showed proficiency, handling the event as a full-blown security breach.

Organizations are reminded to verify that they are using a trusted, competent third party to dispose of devices, or that they are taking all the necessary precautions if handling the decommissioning themselves. That should extend past routers and hard drives to any device that's part of the network. Many organizations in this research probably felt that they were contracting with reputable vendors, but their data still leaked. With this in mind, it's recommended that organizations follow the manufacturer's guidelines for removing all data from a device before it physically leaves their premises, which is a simple step that many IT staff can handle.

Organizations are reminded to treat disclosure notifications seriously. Doing otherwise may leave them vulnerable to a costly data breach and significant reputational damage.

At RSA 2023, Camp and Anscombe will present this research at the presentation "We (Could Have) Cracked Open the Network for Under $100" on April 24, 2023, at 9:40 a.m. PT.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant
Vistar Communications

+971 55 972 4623
email us here