CISO MAG

beyond cybersecurity

Volume 4 | Issue 08 | August 2020

UNDERSTANDING THE IoT THREAT LANDSCAPE

XDR IS HERE

Unknown threats detected and automatically stopped over time by Trend Micro. Created with real data by artist Brendan Dawes.

Threats are evolving. EDR is not enough.

The latest threats have been engineered to hide from your standard detection and response security.

Security and SOC teams are suffering from alert fatigue, lack of visibility, and difficulty with integration from siloed solutions.

We're staying one step ahead.

Trend Micro™ XDR gives your organization the ability to detect and respond to threats faster, across email, endpoints, servers, cloud workloads, and networks.

When you can correlate alerts and information from multiple vectors to effectively secure your organization - That's The Art of Cybersecurity.

AI Security Analytics

Beyond the Endpoint

Complete Visibility

Learn more at Trendmicro.com/XDR

TREND MICRO™

CISO MAG
beyond cybersecurity

Volume 4 | Issue 8
August 2020

Image credits: Shutterstock
Cover & Layouts by: Rajashakher Intha

EDITOR'S NOTE

ESTABLISH A SECURITY BASELINE FOR IoT

The saying that Internet connectivity is the "electricity of the 21st century" is truer than ever today as we are all locked away in our homes. Yet, we are on the cusp of another Internet revolution that connects "things" and not people or their computers. In 2010, Hans Vestburg, the former CEO of Ericsson, declared that 50 billion things would be connected to the Internet by 2020. With the rate at which digital transformation is happening today, I think this number could be much more than that. The introduction of 5G networks will see a further jump in IoT devices in the next two years.

Things with embedded sensors — smart home devices, industrial machinery, agricultural soil probes, modern health care equipment, even cars, spacecraft, and airplanes — are all connected to the Internet. Further, critical infrastructure such as energy grids, nuclear power plants, transportation networks, communications networks, are systems and assets essential for the functioning of a society or an economy and they are vulnerable to attack just like anything else in the digital age.

We all know that the security of Critical Infrastructure (CI) and any connected device can be compromised. There are many stories of CI vulnerabilities and breaches, some of which you can read in the articles within this issue. In fact, a research group called the X-Force at IBM have monitored attacks on industrial systems and reports a 2,000% increase since 2018.

IoT devices' compromised security puts the economy at risk. Back in 2015, it was predicted that machine-to-machine communications alone would generate approximately US$900 billion in revenues by 2020.

But it is not only the economy that could be impacted. Nations are also targeting the CI of other countries through IoT attacks. Policymakers, business leaders, and governments must recognize this and realize that the IoT landscape is a highly lucrative target for bad actors and rogue nations.

Read our Cover Story and other IoT articles in this issue to put all this in perspective.

We hope you are safe and well.

Please write to us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief

INDEX

Chronicle

Detect, investigate and hunt at Google speed

Chronicle, now part of Google Cloud, is a security analytics platform that works at planet-scale. Redefine your SIEM with zero-management security analytics from Chronicle and let us ensure perfect fidelity, no matter how much data you generate.

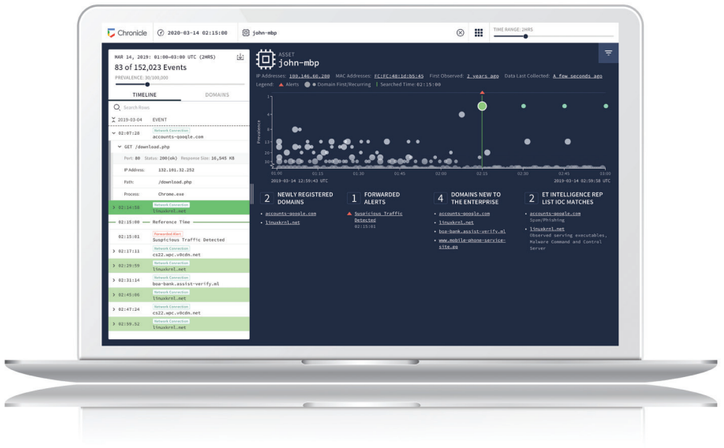
Get a free TCO impact analysis

In 15 minutes we will produce a detailed cost comparison between your legacy SIEM and Chronicle that you can download and use for your own internal analysis.

Sign-up today:

https://chronicle.security/unwind-your-siem

Modernize your enterprise security with Chronicle.



Google Cloud

CYBERSECURITY

TOP 5 LESSONS LEARNED FROM COVID-19

- Hemanta Swain,
VP, & CISO at TiVo Corp

At last, I went to a grocery shop with enough precautions after using multiple online delivery services for weeks. And I found that most people are following health advice and keeping safe distances, although it makes it hard to recognize anyone wearing a mask. This was, and still is, an unusual experience for everyone. COVID-19 is the biggest challenge that we face today. The COVID-19 pandemic has forced us to stay home to save lives and has given us time to rethink our actions and prepare for a healthier future.

Through my personal experiences and learning from COVID-19, I realize that this pandemic resonates closely with my Infosec professional life. This may not be new for cybersecurity professionals, but I will outline a few of my experiences here.
In the minds of many people, this transition from physical to digital is inevitable, unstoppable, and irrevocable, even though cash is still used for most retail purchases globally (COVID-19 influence aside).

1. **Basic (Health/Security) Hygiene:**
   The pandemic has reminded us all that the most basic of hygiene strategies, handwashing, first to be discovered to be effective against spreading disease in the 1850s, is still one of the most important ways to stop the spread of diseases in 2020.

   As for cyber security, we should be reminded that basics cannot be ignored in our industry either. It's not uncommon to see security professionals lagging behind in the adoption of the latest technologies that address challenges (advanced threats) and support business priorities. We are also reminded of the number of breaches that happen because of haphazard patching and other basic requirements not being met. Just like with handwashing, all cybersecurity professionals know that keeping up to date with patches is key to protecting the organization from easily avoided breaches. Moreover, we tend to overlook the basic health of our infrastructure, systems, and applications. This becomes evident during a security breach.

   In my view, both are needed, but there should be a continuous effort to keep basic security hygiene intact. This is essential to build a sustainable security posture. One can and should follow CIS top 20 controls and OWASP top 10 list with secure access using multi-factor-authentication, regular patching, vendor risk assessment, email security, and endpoint security protection. But basic security hygiene is the key.

2. **Segmentation (Shelter-in-place and Isolation):** During this pandemic, we've seen, perhaps for the first time, the entire world sheltering in place simultaneously. We've seen how isolating people from their networks of friends and extended family drastically helps contain infection rates.

   The parallels in cybersecurity are obvious: understand your business, infrastructure, applications, and the most valuable assets. Appropriately segment your network, systems, and applications to allow access to only those who require it. This is beneficial to minimize impact during a crisis, allowing you to contain any breaches, and will be a foundation for your zero-trust framework.

3. **Security (Health) Leadership and Culture:** If this pandemic has taught us anything, it's that when health leaders, politicians, and local culture are in line with best practices for limiting the spread of the disease, the effects of COVID-19 are minimized more quickly and with fewer deaths. When messaging to the public is unclear, valuable time is lost and local culture doesn't shift quickly enough to impact results.

   For cybersecurity, it's imperative to clearly define roles and responsibilities to take appropriate ac- a timely manner, especially during a cri- adership helps to build a securi- ch is essential to reduce risk Yes, there is no infinite bottom line and

Vol 4 - Issue 08