



chronicle

2020

Global expertise helps build a safer world

kaspersky

BRING ON
THE FUTURE

Global network of world-class analysts informs threat intelligence reporting service, providing unique, actionable insights for Chronicle's security intelligence efforts

Chronicle's mission is to 'give good the advantage', by helping businesses win the fight against cybercrime.



Cybersecurity

- Headquartered in Mountain View, California
- Part of the Alphabet family (now part of Google Cloud)
- Kaspersky Advanced Persistent Threat Intelligence Reporting

“Kaspersky is often the first to identify when a new threat is emerging, even before the software manufacturers know anything about it.”

Juan Andres Guerrero Saade,
Researcher, Chronicle Security

Chronicle launched as an Alphabet company in 2018, applying unique resources and talent to its goal of giving organizations, and the people within them, the tools to protect their critical infrastructure and systems from global cybercrime.

It applies global computing and analytical power to enable enterprise security teams to identify cyber threats before they cause harm.

Challenge

Whatever your favorite source of cybercrime statistics, the scale of cost and damage is eye-watering, alarming and climbing fast. The proceeds of cybercrime are thought to exceed \$1.5 trillion a year and everyone is a potential target, from individual citizens to nation states. One in three Americans falls victim to cybercrime every year.

The global cost of ransomware is predicted to reach \$20 billion in 2020. A typical Denial of Service (DoS) attack can cost a large business more than \$2 million per event. Our phones, computers, cars, bank and credit card accounts, even smart home devices and alarm systems, are all vulnerable to a determined cybercriminal.

Chronicle is a key player in the fight, working with major corporations and government authorities, applying extensive data analytics expertise to help turn the tide and to stop the hackers in their tracks.

Its arsenal of weapons against the cybercriminals includes the means to interrogate vast quantities of security telemetry data from organizations worldwide, and to find unique intelligence and insights about live global threats. The result is a comprehensive investigation service, greatly improving the prospects of outwitting the enemy before the damage is done.

But Chronicle understands that in the war against cybercrime it's vital to enlist cybercrime mitigation expertise to join them in the battle.



2018

launched by Alphabet

2019

core analytics
service launched

Kaspersky solution

Kaspersky Advanced Persistent Threat (APT) Intelligence Reporting service draws on the skills of its Global Research and Analysis Team (GReAT). The team is recognized worldwide for exposing some of the most notorious threat actors and sophisticated cyber espionage campaigns of recent years.

Subscribers to the service receive unique, ongoing access to GReAT's worldwide APT investigations and discoveries, with immediate alerts about imminent threats, backed by detailed reports featuring bespoke, actionable advice and guidance and full technical data.

Using this information, organizations can respond quickly to new threats and vulnerabilities, deploy blocking techniques, change working practices to reduce potential damage and put in place strategies to promote a more secure digital future.

In addition, access is provided to the Kaspersky APT Reporting database, which brings together all the research made by GReAT over the years. This unique resource provides a great opportunity to learn lessons and help build internal security teams' knowledge and skills.

Global telemetry platform

Chronicle's core service is a global security telemetry platform for investigation and threat hunting within an enterprise network. It makes security analytics instant, easy and cost-effective. The service is built on core Google infrastructure, and brings unmatched speed and scalability to securely manage and analyze massive amounts of security telemetry.

For Chronicle researcher Juan Andres Guerrero Saade, having the support of the Kaspersky team provides a vital extra layer of intelligence and expertise.

"What our teams at Chronicle are trying to do, in assessing the vast quantities of telemetry data that businesses produce, is to decide where the true, genuine areas of concern and threat reside and then how we can disrupt them," he says.



Confidence

From the world authority on emerging cyber threats



Speed

Instant access to global experts to buy valuable planning time



Actionable Intelligence

APT Report contains IOCs and Yara rules along with practical advice and guidance



Added Value

By regularly identifying new threats quickly

“We knew these were the sort of questions that the Kaspersky Threat Intelligence Services could help us to answer. Kaspersky has the expertise to tell me about new threats, what’s lurking in the shadows that we’re unfamiliar with, rather than simply giving me a barrage of recycled news that doesn’t add anything new to our understanding.”

Culture of curiosity

Guerrero continues: “What Kaspersky offers is a depth of expertise combined with a volume of telemetry that’s often not available anywhere else. The company also has a level of curiosity, a willingness to explore and a desire to reveal new threats and to consider the global implications of those threats. That’s very unusual.

“Kaspersky is often the first to identify when a new threat is emerging, even before the software manufacturers know anything about it. Being able to talk immediately to the expert who made that discovery, to get an advanced picture of what it looks like, buys us vital time to figure out our response and how best to protect our customers.”

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
www.kaspersky.com/fraudprevention

www.kaspersky.com

kaspersky

BRING ON THE FUTURE

2020 AO KASPERSKY. ALL RIGHTS RESERVED. REGISTERED TRADEMARKS AND SERVICE MARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.