X-Force
Threat Intelligence

GDPR One Year Later

The Unintended Consequence for Cybersecurity

New Data Show the Need for Precision Privacy Regulation

IBM

GDPR One Year Later

The Unintended Consequence for Cybersecurity

X-Force
Threat Intelligence

New Data Show the Need for Precision Privacy Regulation

When the European Union's General Data Protection Regulation (GDPR) took effect a year ago, it represented a much anticipated turning point in data privacy regulation. While it was heralded by privacy advocates, there were also concerns—specifically from the threat intelligence community—about the potential impact of a strict interpretation of the regulation on the ability of law enforcement and security researchers to access vital intelligence used to thwart espionage and other forms of cyber-crime.

Among many others in the industry who raised alarm about this outcome, **Caleb Barlow, Vice President of IBM X-Force Threat Intelligence** detailed those concerns in an article in May of 2018[1], looking at the potential pitfalls of a broad interpretation of the GDPR and how it could impact access to the **WHOIS**[2] database, a public registry of web domains that includes information about who owns and operates them.

When an individual or organization registers a domain—like IBM.com—they provide basic contact information to an accredited registrar. The registrar then provides that information to WHOIS, and it is made publicly available on the WHOIS database, much the same way names, addresses and telephone numbers are published in a traditional phone book.

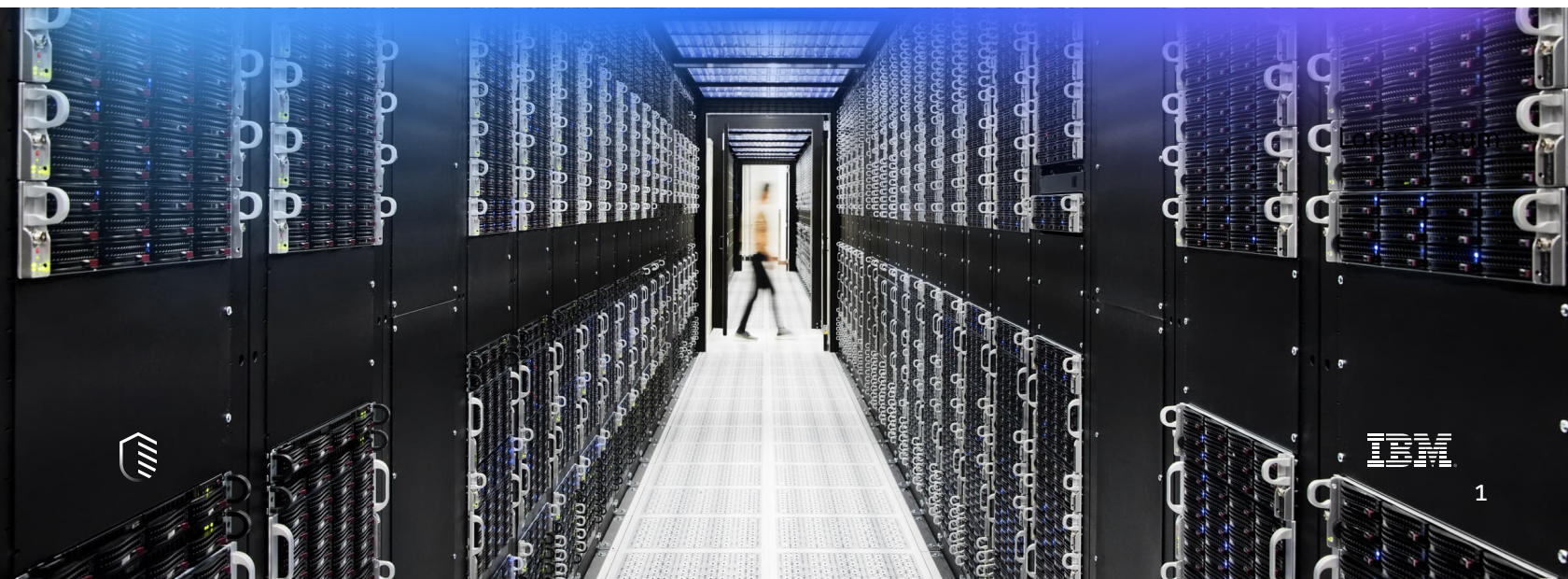
Barlow's May 2018 article goes on to describe how WHOIS data is used by security researchers and law enforcement to keep the web safer, and how losing it could diminish their capacity to protect businesses and the public.

Over the last year, the feared ramifications have become reality. IBM X-Force Threat Intelligence Research now has data that demonstrate the impact GDPR is having on the ability to use traditional WHOIS analytics to track and block malicious domains that are launched by cybercriminals and used to conduct nefarious activity on the web.

There may be consequences beyond cybersecurity, as well. While the research describes the fallout X-Force Threat Intelligence Researchers are seeing, it's important to understand that a similar effect is likely occurring for everyone who uses WHOIS public information to protect their constituents. That includes law enforcement and consumer protection agencies, child advocacy groups, anti-human trafficking organizations, intellectual property rightsholders and others.

[1] **Security Intelligence: https://securityintelligence.com/whois-behind-cyberattacks-under-gdpr-we-may-not-know**

[2] **WHOIS: https://whois.icann.org/en**



GDPR One Year Later

The Unintended Consequence for Cybersecurity

X-Force Threat Intelligence research reveals 91% decline in ability to track and block malicious domains

X-Force Threat Intelligence Research tracked the worldwide number of malicious domains they were able to identify and block using WHOIS data from October 2017 to February 2019.

In the month of October of 2017, researchers were able to use information from the WHOIS database to identify and block about 1.8 million newly registered malicious domains. But as of February 2019, that number had dropped to less than 160,000 malicious domains—a 91% decrease. The drop in the number of identifiable domains (shown as the solid blue line on the chart) corresponds with the decline in domain registrations made publicly available (shown as the solid gold line on the chart) as the GDPR was implemented.

Outside of telling us that publicly available registration information on the WHOIS database has dropped in the past year—and with it, threat researchers' ability to use that information to fight cybercrime—the data may offer us other insights into ways criminals are using this situation to their advantage.

A **November 2017 to May 2018:** This range on the blue line shows that the number of domains researchers could identify as malicious began to drop sharply, correlating with a decrease in the number of records being published publicly to the WHOIS database.

- X-Force Researchers attribute the decline in published WHOIS content to the fact that some domain registrars likely began redacting ownership information from WHOIS, in anticipation of the GDPR taking effect.

B **May 2018 to February 2019:** This range on the blue line shows the number of domains researchers could identify as malicious using the WHOIS database continued to decline. Ultimately, their ability to use WHOIS information was reduced to just 9% of its former effectiveness.

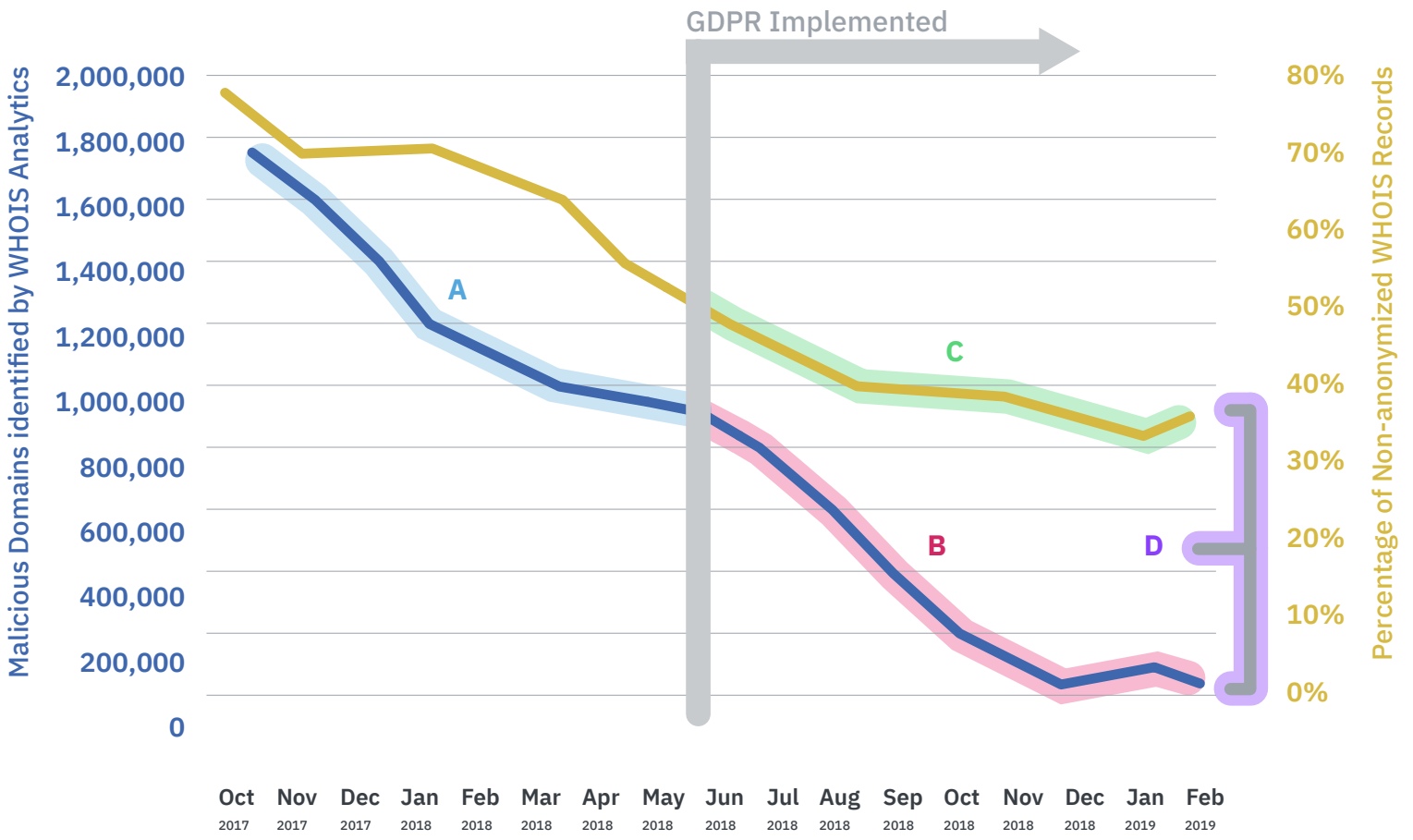
C **May 2018 to February 2019:** This range on the gold line shows that global registration information published to WHOIS also declined, but at a slower rate—levelling off at around 37%.

D **A delta of 28%**: This range between the gold and blue lines—the difference between the 37% of domains that appeared in the WHOIS database versus the 9% researches could identify as malicious—may indicate:

- Cybercriminals—who are keenly interested in keeping their ownership information private—have identified which registrars are redacting ownership information (to comply with the GDPR) and are registering their domains through them.
- Legitimate business and individuals, who do not have a vested interest in shielding their ownership information from the public, are continuing to launch domains with registrars regardless of whether or not a registrar redacts information from the WHOIS registry.
- As a result, the 37% of public registration data available on the WHOIS registry is largely from legitimate organizations and individuals—because **cybercriminals have identified a virtual safe-haven** inadvertently provided by registrars who redact ownership information from WHOIS as they seek to comply with the GDPR.

Cyber criminals may be distorting the intent of the GDPR, identifying a loophole and using it to their advantage. In the process, they gain not only invisibility to law enforcement and security researchers, but also more time to conduct their schemes and more freedom to prey on victims.

GDPR Impact on Malicious Domain Identification and WHOIS Records



Achieving privacy at the expense of security is not sustainable. Organized criminals — and that is exactly who is behind an estimated $600 billion annual cybercrime business—are smart, sophisticated, and opportunistic. If there are proverbial holes in the fence, they will find them, and they will use them.

What is not in question here is the intent of privacy laws—to safeguard the public's online privacy. But this also calls into sharp contrast the need for balanced approaches to data privacy that fix the real problem while avoiding unintended consequences.

The security industry is continually innovating—driven largely by Artificial Intelligence (AI)—and evolving new ways to help protect clients, even with limited WHOIS data accessibility. But our best line of defense is always our most obvious one. Reestablishing access to the WHOIS registry for the legitimate purposes of cybersecurity and law enforcement would put security researchers, and those we seek to protect, in a much stronger position.

We may otherwise unintentionally be giving online adversaries the anonymity they need to elude detection—and that ultimately could pose a serious security threat to the very data we seek to protect.