eBook

Ransomware: How to Regain Lost Ground

Datto's Ryan Weeks on Repelling the Surge in Destructive Attacks

datto

iSMG
INFORMATION SECURITY MEDIA GROUP

Ryan Weeks

Amid a surge in destructive ransomware attacks, Datto CISO **Ryan Weeks** says we "are losing ground" to the adversaries. He offers insight from a new Global Ransomware Report and the start of a multisector Ransomware Task Force.

In this video interview with Tom Field of Information Security Media Group, Weeks discusses:

- Datto's role in the Ransomware Task Force;
- Why he believes we "are losing ground";
- How enterprises can better protect themselves against the latest attack trends.

As chief information security officer, Weeks is responsible for directing and managing Datto's information security program. He spent 11 years securing enterprise applications, systems and sensitive customer financial data at FactSet Research Systems, where he orchestrated all facets of the global information security program.

A Multisector Ransomware Task Force

TOM FIELD: Datto has become a founding member of the multisector Ransomware Task Force. What can you tell us about this task force, and why is it important for Datto to be in there on the ground level?

RYAN WEEKS: The Ransomware Task Force was founded in December 2020 by a core set of companies that wanted to collaborate more broadly, bringing policy, legal, insurance and technology experts from across the globe together to work quickly and determine what we can do to reduce the rate of occurrence of ransomware attacks. When Datto heard about this, we told the folks at the Institute for Security and Technology that we needed to be in on it.

That's because we're in the trenches with managed service providers, or MSPs, every day, fighting the ransomware fight and helping them and customers recover from ransomware attacks. We have a really good pulse on what's happening in the small and medium businesses and enterprises and with MSPs as a whole, and we want to make sure that whatever this task force comes up with is going to benefit small and medium enterprises, or SMEs, and small and medium businesses, or SMBs, just as much as it does large enterprises and government institutions.

Losing Ground to Ransomware Attackers

FIELD: In a recent blog that you wrote, you said that we're losing ground to the adversaries. Can you go into depth on that, please?

WEEKS: At a minimum, we can agree we're not gaining ground. Every year, year over year, more ransom is paid than in the prior year. The continued success of attacks and the rate at which we're hearing about attacks is definitely going up. And attacks have slowly become more targeted instead of opportunistic. We still see opportunistic attacks, but ransomware as a service is creating a very strong business model for threat actors. We see more and more of it.

In terms of holding ground, advancing or retreating, we're losing ground. Why is that? One reason is that we're all in our silos, trying to fight the fight in our individual industries. That's why Datto jumped onto the Ransomware Task Force. It's exactly what we need. It's the right thing, with the right set of people, with the right objective, at the right time.

Troubling Ramsomware Trends

FIELD: We're seeing a lot more targeted attacks and more destructive attacks. Based on Datto's recent Global Ransomware Report, what specific ransomware trends give you the most concern?

> "Attackers have gotten better at picking their targets. They're not going for breadth; they're going for depth."

WEEKS: My top concern is that SMBs are not overly concerned about ransomware relative to service providers. They either think, "I'm too small. I'm not even on an attacker's radar," or they have an "it won't happen to me" mentality. MSPs are incredibly concerned, because they're seeing and living it. Their businesses depend on their ability to persist through attacks and to get their customers through them.

My second concern is that, this past year, while MSPs saw less ransomware, the amount of ransom requested and the cost of the downtime went up. That means the attackers have gotten better at picking their targets. They're not going for breadth; they're going for depth. They want to monetize a target as much as they can and make it hard for that target to recover without paying a ransom. The data supports that MSPs and SMBs are seeing this trend.

A Takedown Is Just a Reprieve

FIELD: Ryan, in news recently, we've seen some high-profile takedowns and even the retirements of some of the so-called ransomware families. What do these developments mean?

WEEKS: You want to be encouraged by them, but these threat actors still exist. Maybe their infrastructure or their specific software has been taken down, but we've seen that before. We've seen large takedowns of botnets and exploit kit infrastructure and ransomware groups, and those takedowns give you a brief reprieve. But you can almost guarantee they'll be back, in one form or another. A takedown buys you breathing room and a bit more time to work on your preparedness for these threats, but it shouldn't be viewed as the answer to the problem.

We should definitely keep trying to do takedowns, because they are an essential piece of the problem. But it's playing whack-a-mole. There are many difficulties with taking down some of the distributed infrastructure and architecture that supports these threats. Takedowns are not the answer to the whole problem.

> "Cyber resiliency is the ability for a business to continue to operate through an adverse cyber event with the least possible amount of damage and loss."

The Goal Is Cyber Resiliency

FIELD: How can Datto's customers better protect themselves and their customers from this surge in destructive ransomware attacks?

WEEKS: Ransomware makes us look at cyber preparedness or cyber resiliency. Cyber resiliency is the ability for a business to continue to operate through an adverse cyber event with the least possible amount of damage and loss. Ransomware is purely destructive. It's as bad as it gets in terms of an attack. A ransomware attack should be considered synonymous with a data breach. We know attackers are in these infrastructures for days, weeks and months ahead of the actual ransom event, and they're in there stealing data.

If you don't pay the ransom, they're going to try and extort you by making sensitive documents, intellectual property or personal data of your customers available to the public. You need to improve your security program and your cyber resilience. A lot of people use the NIST framework – identify, protect, detect, respond, recover – and focus on the identification and protection components of a ransomware attack. But to become more resilient, we need to have stronger capabilities to detect, respond and recover from these threat actors.

Customers need to look at how they're developing capability across the entire spectrum of identify, protect, detect, respond and recover. Notice that I said "capability"; I didn't say technology or controls. Capability means a combination of people, process and technology that supports cyber resilience, not just tools and technology. Capability includes strong business continuity and incident response. In the cyber defense matrix, the recovery and response categories require strong people and process, and that's where we need to focus a lot more energy. We need to stop relying on tools and start looking more at people and process as capabilities and invest in them. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® Just for Credit Unions GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk® TODAY CAREERS INFO SECURITY® Data Breach. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io