Q&A

WEBROOT®
Smarter Cybersecurity™

The Truth About Crypto Ransomware

Crypto ransomware is making headlines, lurking in ads on popular websites and shutting down hospitals. Where and when did crypto ransomware burst onto the scene, and what does the future hold? In this Q&A, Hal Lonas, Chief Technology Officer at Webroot, looks at the evolution of crypto ransomware, what can be done to protect customers, and whether the FBI is right in advising victims to pay the ransom.

Q: How have you seen crypto ransomware evolve over time?

A: In the early days of CryptoLocker, back in September 2013, we were very good at detecting and/or remediating the impact of crypto ransomware. At that time, it was quite rare, but we've watched it advance steadily in both sophistication and impact. Now, we have an in-house team focused on keeping our efficacy against crypto ransomware as high as possible, and we closely monitor for any successful intrusions against our defenses.

Crypto ransomware is now at the ransomware-as-a-service stage, where any cybercriminal can get their hands on encrypting ransomware variants and set up shop in the extortion business. Its prevalence is widespread and it's getting more difficult to stop.

Q: How can MSPs protect their customers from crypto ransomware? What can they do to ensure the most protection?

A: We are in the process of publishing a technical white paper on this. While having a highly effective endpoint antivirus/antimalware solution in place is absolutely essential, there are a number of other mitigation strategies that are equally important. Some of these involve Windows system settings, email server settings, and restricting certain rights, but the best way to protect customers is to have both a great endpoint security product and solid backup and recovery procedures.

Businesses need a backup solution for disaster recovery and business continuity, but now, with crypto ransomware, it's more important than ever that the backup be secure. If held hostage, even when an organization pays the ransom, there's no guarantee they'll get their data back easily or intact, and they may be targeted continually thereafter as an 'easy mark'.

Q: Do you know of any product that is 100% effective against crypto ransomware?

A: I would love to say Webroot is, or even privately name a competitor, but the truth is: no, I do not.

I do know an endpoint security solution that is 100% in most cases, from an organization that is focused on making it 100% all of the time, and I'm proud to say that it's Webroot. I honestly believe we are best placed to minimize the impact for both our services partners and customers. Unfortunately, the nature of our business means there are no 100% guarantees on effectiveness.

The fact is—no matter how proactive and effective you are today—attackers have the advantage and can test your defenses from a variety of threat vectors. That's why security has always been about different layers and mitigation approaches. To mitigate crypto ransomware, you need more in-depth defenses.

Q: Do you believe the FBI is correct in advising people to pay the ransom?

A: No, my personal belief is that the FBI is not right to recommend that course of action. It's a lazy approach to something that is fast becoming a major disruption for businesses of all sizes, but particularly small businesses that do not have the backup regimens or recovery resources of larger enterprises.

The FBI are right, however, to state that paying up is the only practical way to get your data back once it has been encrypted, if you don't have the ability to clean up the threat and restore the encrypted data yourself. But it's important to bear in mind that even paying up doesn't guarantee you'll get your data back, even though it works in most cases.

Q: What should you do if your customers become infected by crypto ransomware? Should you pay the ransom?

A: I've touched on that in the last response. If corporate data is valuable and core to your business and you suffer a breach, then I'd recommend getting your defenses ready to thwart future ransomware demands, but also paying the ransom promptly. Usually, the ransom amounts increase the longer you wait.

If you pay, it's highly likely you'll get the encryption key and instructions to unlock your data and whatever other items attackers have hidden there. Without the decryption key, your data is unrecoverable. That's why the proactive security and recovery strategies I've talked about are so important.

Q: Are there any new trends with malware and crypto ransomware that MSPs should be on the lookout for?

A: The trend in crypto ransomware is that it's becoming more and more common, and will continue to target businesses and consumers who don't have great endpoint security and a great backup strategy. Apple® Mac OS X is now being targeted by KeRanger, and Locky for PCs has already changed its propagation from Microsoft® Word file macros to JavaScript, while a new ransomware variant called Cerber has shown up too.

These developments have all come in 2016, and we're barely into March as we have this discussion. Since the trends don't show any signs of slowing down, MSPs should prepare for the worst by ensuring they take all practical measures to lock down and secure clients' systems and data, and help their clients implement appropriate recovery practices in the event of a successful ransomware attack.

About Webroot

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks. Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
800 772 9383

Webroot EMEA
6th floor, Block A,
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0)870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900