Ransomware incidents jump in Q3
MSPs and their small business clients are targeted

Targeting of IT vendors by cyber criminals contributed to a 37% increase in reported ransomware incidents in the third quarter of 2019 compared to the previous three months.

In fact, of the ransomware incidents reported in Q3 to Beazley's in-house breach response team, Beazley Breach Response (BBR) Services, 24% were confirmed to be caused by a vendor or managed service provider (MSP). Small businesses, which often rely on MSPs to remotely manage their IT infrastructure, reported 63% of all ransomware incidents to BBR Services in 2019. And though a business' level of reliance on its MSPs can vary, with some using an MSP to support their own internal IT resources, many small businesses outsource their entire IT operation to the MSP, from building the network, managing applications, and servicing any and all IT requests. This can create a dependent and deeply interconnected relationship that hackers sought to capitalize on in Q3.

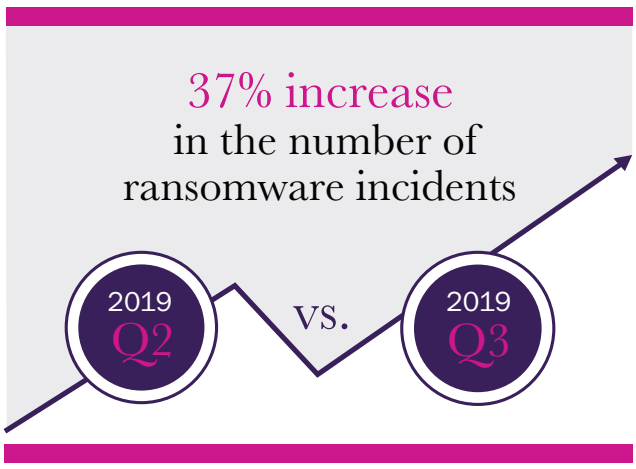
MSPs make for ripe targets for ransomware attacks. Joshua Dann, incident response practice lead at Lodestone Security, a wholly owned subsidiary of Beazley plc that was created to provide cybersecurity consulting services tailored to the small and mid-sized business market, observes "MSPs have to balance a need for speed and convenience when it comes to being able to respond to clients, with ensuring the right security controls are in place. Too often, speed and convenience win out over security controls." For example, in many cases, MSPs have reused credentials across clients so that MSP employees can service multiple clients more quickly. Similarly, MSPs might not enable multi-factor authentication (MFA) on the remote access point they use to pivot to client environments.

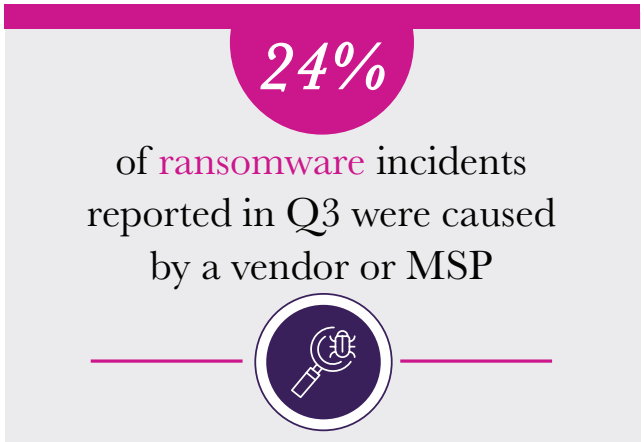
In almost all of the MSP ransomware investigations for downstream clients that Lodestone managed in Q3, attackers exploited the remote management application that connects the MSP to the client. The same MSP user account would log into multiple client environments and install ransomware. If the MSP had set up individual user accounts for each of its clients, it is more likely that the exploitation of the single set of credentials would have only enabled unauthorized access to a single client's environment. Further, an MSP user account often has to have full administrative access in order to assist with regular IT functions, so when credentials were compromised, the attackers had full administrative access to clients' environments.

So, why the increase in MSP ransomware attacks this summer?

According to Bill Siegel, CEO and co-founder of ransomware response platform Coveware, "Attacks on MSPs are not new, as the attack groups behind GandCrab previously targeted MSPs to magnify the impact of an attack." But this summer the threat has increased. Siegel adds, "Developers of Sodinokibi ransomware appear to have applied lessons learned from GandCrab MSP-infection pain points to make the attacks more profitable."

MSP ransomware attacks this summer exposed unique incident response challenges. For small businesses who completely rely on outsourced IT, a massive ransomware attack across clients draws on the MSP's resources and inevitably leaves many businesses in the dark. Small business owners without a technical background struggle to understand and assist external legal and forensics vendors





BZCER022_US_10/19

hired to help them respond to the attack. The response is further complicated when the MSP itself is also infected with ransomware. Where an attack group knows they have hit an MSP, and also infected downstream clients, they may refuse to negotiate with the end clients and instead only respond to the MSP in order to increase their ransom demands. This tactic can also leave clients with little to no control over their data software recovery.

About Beazley's BBR Services Team

Beazley has managed thousands of data breaches since the launch of Beazley Breach Response in 2009 and is the only insurer with a dedicated in-house team focusing exclusively on helping clients handle data breaches.

The BBR Services team works directly with BBR insureds during all aspects of incident investigation and breach response and coordinates the expert services that BBR insureds need to satisfy legal requirements and maintain customer confidence. In addition to coordinating data breach response, BBR Services maintains and develops Beazley's suite of risk management services, designed to minimize the risk of a data breach occurring.

If your organization uses an MSP as its IT solution, Lodestone recommends strong controls around the central server that the MSP uses to access your environment. In vetting a potential MSP, consider asking the following:

MSP checklist

- Is there a security program in place, including periodic risk assessments to identify areas for improvement?
- Is there ongoing security awareness training across the organization?
- Is there a SSAE 18 SOC 2 Type II report or similar type of report available to customers, attesting to security control environment?
- If access to personally identifiable information or protected health information is necessary, how is this protected at the vendor (e.g. encryption, secure remote connections, restricted access, logging and monitoring)?
- Are security and availability requirements enforced in master service agreement contracts (e.g. sensitive data protection, uptime guarantee / service level agreements, security incident reporting / coordination, regulatory compliance requirements)?

beazley

www.beazley.com/bbr