8 Security Actions for Tyler Technologies Customers

The September 2020 data breach at software provider Tyler Technologies is a Call to Action for their Government and Public Sector Customers

Michael K. Hamilton, CISSP
Chief Information Security Officer | Critical Insight

A large technology service provider to local government in the United States has been hit by ransomware[1] and every customer likely needs to take action.

Tyler Technologies provides a variety of on-premise, cloud, and hosted applications that facilitate government operations from law enforcement to finance.

Security experts in the Public Sector predict the fall-out will continue for months to come. While the full story and impacts are still unfolding, there are remediations that customers who use Tyler Technologies' products should take right now to protect and defend their networks, critical systems, and data.

Critical Insight convened a panel of experts in local government on September 30, 2020, to go over what we know about the breach today and what security teams can do now. Read on for the summary of that discussion and the top eight security actions that were called out as mission-critical for Tyler Technologies' public sector customers.

© 2021 Critical Insight Inc.

What We Know About the Tyler Technologies Breach

Sourced from published reports and personal experience.

- Tyler Technologies has been hacked with ransomware.
- Information published by the company is unspecific and does not address questions about what actors with persistence could have accessed.
- One of our consulting customers brought the lack of 2FA and unmanaged logins to our attention.
- It has been reported that Tyler credentials have been used for unauthorized access.

What We Understand About Tyler Technologies Products

Including information from one penetration tester that has performed multiple assessments on Tyler products, albeit two years ago.

- For Tyler Connect customers, 1433 was found open to Tyler.
- Brute force against SQL admin credentials suggests bad credential management; note this is a report from two years ago.
- Tyler required 3389 to be open to the Internet for RDP.

What We Can Surmise and Possible Implications for Tyler Customers

- Actors may have had persistence in the Tyler network, considering the available evidence and average dwell time of a threat actor (200+ days).
- IF observed practices have persisted, then credentials may have been insecurely stored and thus lifted.
- It is possible that open SQL connections were used to exfil data from Tyler Connect customers.
- It is also possible that stolen admin credentials have been used to log into MUNIS systems and gain further access, potentially dropping further ransomware into government networks.

© 2021 Critical Insight Inc.

8 Security Actions for Tyler Technology Customers To Do Now

1. Lock out Tyler logins if you have not already.
2. Determine at the firewall if any Tyler-specific rules are in place, and if they include 1433 and/or 3389.
3. Especially if those ports are open, check application and database logs for unexplained data transmissions or activity on RDP.
4. Focus monitoring on Tyler applications.
5. Review MUNIS and Tyler Connect application logs for unexplained logins. If there have been unexplained connections or data transmissions, begin scanning systems with a product that is different from the one you're using for endpoint protection now. If there are lurking malware or control bots, you'll need to find them quickly.
6. If you suspect that unauthorized actors have accessed these systems or exfiltrated data, run a security detection tool on suspected systems. If results inconclusive, consider re-imaging.
7. Suspicious log entries should be preserved and federal law enforcement contacted with findings[2]. Try to preserve evidence[3] using best practices in digital forensics - or hire an outside security firm with experts in computer forensics to assist in the investigation.
8. Check with your organization to see if you've worked with Tyler on an upgrade. If so, you may have uploaded a database to the Tyler FTP site or other share location, and they may have had custody of your data during the ransom event. Check your records for proof of destruction/removal.

---

[1] Tyler Technologies and the Threat to Local Government. https://www.criticalinsight.com/resources/news/article/tyler-technologies-and-the-threat-to-local-government

[2] 3 Methods to Preserve Digital Evidence for Computer Forensics. https://www.criticalinsight.com/resources/news/article/3-methods-to-preserve-digital-evidence-for-computer-forensics

[3] Forensic Analysis of Digital Media – 4 Methods Explained. https://www.criticalinsight.com/resources/news/article/forensic-analysis-of-digital-media-4-methods-explained

© 2021 Critical Insight Inc.