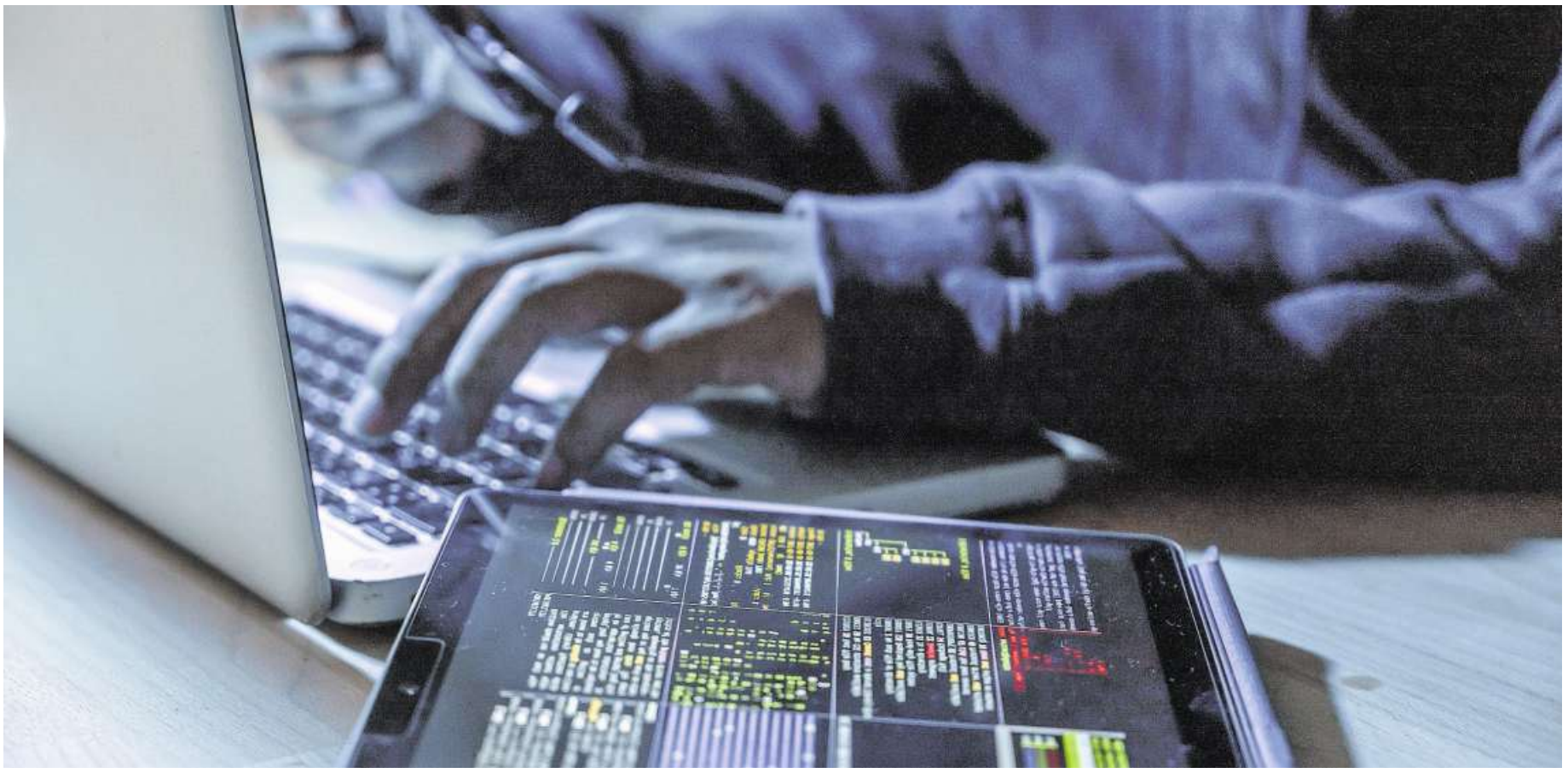

Hacker haben bei den Basler Behörden zugeschlagen, eine grosse Menge an Daten aus dem Erziehungsdepartement entwendet und ins Darknet gestellt. Bild: Getty Images

«Andere Gangs könnten folgen»

IT-Experte Marc Ruef äussert sich zum Fall der gestohlenen Daten aus dem Basler Erziehungsdepartement.

Interview: Daniel Schurter (Watson) und Jonas Hoskyn

Am Mittwoch wurde publik, dass rund 1,2 Terabyte Daten des Basler Erziehungsdepartements im Darknet zugänglich sind. Es ist die «Beute» von Cyberkriminellen, die mit ihrem Erpressungsversuch scheiterten und die Daten quasi als Bestrafung des zahlungsunwilligen Opfers publizierten. Hinter dem massiven Datendiebstahl steckt eine Gruppe, von der die Öffentlichkeit bislang relativ wenig weiss. Der Schweizer IT-Sicherheitsexperte Marc Ruef, ein profunder Kenner der Ransomware-Banden, hat sich mit «BianLian» beschäftigt und ordnet den aussergewöhnlichen Fall ein.

Herr Ruef, die Attacke auf das Basler Erziehungsdepartement wurde Ende Januar publik gemacht. Dass die Erpresserbande «BianLian» dahintersteckt, ist erst seit dieser Woche bekannt. Was ist an dieser Gruppierung besonders?

Marc Ruef: BianLian hat früher ein klassisches Ransomware-Modell umgesetzt, bei dem Daten verschlüsselt und so Geld erpresst wurde. Jüngst wurde bekannt, dass man sich nur noch auf die Exfiltration, also den Datendiebstahl konzentrieren möchte. Dadurch hat die Gruppierung die Komplexität ihrer Angriffe verringert. Aber auch den eigenen Hebel im Erpressungs-Ansatz verringert. Sie spekulieren darauf, dass eine Veröffentlichung der Daten schmerzhaft genug sein wird, um eine Zahlung durch die Opfer zu erzwingen. Das Vorgehen von BianLian ist in seinen Grundzügen sehr professionell und effizient. Die erbeuteten Daten umfassen oft mehrere Terabyte und kommen einer vollumfänglichen Kompromittierung gleich.

Bereits seit Mitte Januar gibt es einen sogenannten Decryptor, das ist ein Hilfsprogramm, um die von BianLian verschlüsselten Dateien zu entschlüsseln. Dieses von der IT-Sicherheitsfirma Avast veröffentlichte Gratis-Tool dürfte auch der Grund dafür gewesen sein, dass die unbekannten Kriminellen ihre Vorgehensweise grundlegend geändert haben.

Durch das Vereinfachen ihres Geschäftsmodells kann die Gruppe ihre Ransomware simpler strukturieren und sie ist dadurch weniger fehleranfällig. Dass eine Gruppierung das Prinzip der doppelten Erpressung (‹Double Extortion›) aufgibt, ist sehr ungewöhnlich. Aber falls der Erfolg ihnen recht gibt, könnten andere Ransomware-Gangs diesem Beispiel folgen.

Die Malware ist in «Go» programmiert, was bringt das den Kriminellen?

Go ist eine Programmiersprache, die sich zunehmender Beliebtheit erfreut. Sie ist relativ einfach zu erlernen, klar strukturiert und bietet eine Vielzahl vorgefertigter Module, wie zum Beispiel die Verschlüsselung. Der langfristige Vorteil von Go ist, dass sich Programme einfach auf verschiedene Betriebssysteme kompilieren lassen. Es würde also nicht erstaunen, wenn die Gruppierung auch andere Plattformen wie Linux und macOS ins Visier nehmen wird. Momentan scheint man sich aber, wie viele andere Ransomware-Gangs, auf Windows zu fokussieren.

> «Man sollte Cyber-Sicherheit ernst nehmen.»

Marc Ruef
IT-Experte

Was weiss man über die Herkunft der Kriminellen?

Bei unseren Recherchen zu BianLian fiel auf, dass in der bisherigen Berichterstattung im Gegensatz zu anderen Ransomware-Akteuren nie von Russland die Rede ist.

BianLian gilt als relativ junge Gruppierung, die Ende 2022 das erste Mal von sich reden machte. Im Gegensatz zu vielen anderen Ransomware-Gangs scheint es sich nicht um eine Neuformierung durch Mitglieder anderer Gangs zu handeln. Ihr Verhalten zu Anfangszeiten war relativ ungestüm und durch ‹Anfängerfehler› begleitet: fehlerhafte Netzwerkzugriffe, träge Verhandlungen mit Opfern und eine schlechte Erreichbarkeit ihrer Tor-Seite. Über die Herkunft wird noch immer gerätselt. Gewisse Sicherheitsfirmen meinen, Verbindungen zu Nordkorea identifiziert zu haben. Unsere eigenen Abklärungen zeigen Überlappungen mit Akteuren aus Russland, China, Deutschland und Spanien. Eine sichere Zuordnung ist momentan noch nicht möglich. Die bisherigen Opfer finden sich hauptsächlich in Nordamerika, Westeuropa, Australien und Indien. Südamerika, Afrika und Eurasien stehen vorerst nicht im Fokus. Ob das an geopolitischer Ausrichtung, sprachlichen oder kulturellen Hürden liegt, kann momentan nicht gesagt werden.»

Was wissen wir über die geleakten Daten, die Basel-Stadt betreffen?

Wir haben nur die Pfadstrukturen analysiert und vereinzelte ‹Plausibilisierungen› vorgenommen. Wegen unseren ethischen Grundsätzen sowie aus Datenschutzgründen schauen wir keine persönlichen Daten an. Die Sichtung hat gezeigt, dass es sich um «858 ZIP-Dateien» handelt, also komprimierte Daten, wobei «pro Datei ein kompromittiertes Windows-System» gegeben ist. Die Angreifer haben jeweils einen Datensatz eines Windows-Systems heruntergeladen. Diesen haben sie dann in eine ZIP-Datei gepackt, wodurch die Daten einzelner Systeme unkompliziert und effizient ausgetauscht werden können. Dieses Vorgehen ist nicht üblich, da die Leaks traditionell als ein grosses Archiv angeboten werden.

Die unbekannten Cyberkriminellen bekunden aber offenbar Mühe, die im Darknet zugänglich gemachten Opferdaten über einen funktionsfähigen Server anzubieten.

BianLian ist seit jeher für eine schlechte Infrastruktur bekannt. Das Herunterladen ist langwierig und nervenaufreibend. Es braucht verschiedene Anläufe.

Wie schlimm ist das Daten-Leak? BianLian behauptet auf der eigenen Leak-Seite, dass beim Hackerangriff auf das Erziehungsdepartement «HR-, Finanz-, Buchhaltungs-, Studenten- und Mitarbeiterdaten» erbeutet wurden.

Die Pfadstrukturen deuten auf Mitarbeiter, Lehrer und Schüler hin. Es finden sich ebenso gewisse Vertragsinformationen und sogenannte NDAs mit externen Partnern, also Vertraulichkeitsvereinbarungen. Stichproben zeigen, dass hier die Desktop- und Datei-Ordner von einzelnen Personen erbeutet wurden. Es scheinen also Arbeitsplatzrechner kompromittiert worden zu sein oder die Netzwerkfreigaben, auf denen die Benutzerdaten abgelegt sind. Dort finden sich dann die lokal abgelegten Dokumente. Die Datenmenge ist stark davon abhängig, welcher User wie viele Dokumente, Bilder, OneNote-Notizen etc. gespeichert hat. Inhalte des Windows-Papierkorbs sind ebenfalls vorhanden. Ebenfalls finden sich im Browser gespeicherte Passwörter und Formulardaten.

Kann man aus den oben erwähnten fast 860 ZIP-Dateien schliessen, dass es sich um eine entsprechende Zahl von PC-Usern handelt, die vom Leak betroffen sind?

Ja, das lassen die Stichproben vermuten. Das sind die direkt betroffenen Benutzer. Da werden aber auch noch Kundenbeziehungen drin sein, was zu indirekt Betroffenen führen wird.

Wie gross ist das Risiko von weiteren Angriffen?

Historisch gesehen nutzt die Gruppe die ‹Schwergewichte› publizierter IT-Schwachstellen. Also solche, die sehr grosse, bekannte und exponierte Produkte betreffen. Das sind genau jene Schwachstellen, die in der Cybersecurity-Branche sofort zu reden geben und es manchmal selbst in die Tagespresse schaffen. Dies zeigt sehr konkret, dass man das Thema Cybersecurity ernst nehmen und neue Schwachstellen schnellstmöglich adressieren sollte. Nur so kann das Zeitfenster für erfolgreiche Angriffe minimiert werden. Wer das nicht tut, könnte schon morgen ein lohnendes Opfer von BianLian oder einer anderen Ransomware-Gang werden.