SE Labs

INTELLIGENCE-LED TESTING

Breach Response Test
Schutzmodus

BlackBerry Protect und Optics

Juli 2021

SE Labs hat **BlackBerry Protect und Optics** intensiv getestet und dabei reale Hackerangriffe simuliert. Hierbei kamen dieselben Techniken zum Einsatz, die Cyberkriminelle aktuell nutzen, um Systeme zu kompromittieren und sich in Zielnetzwerke einzunisten.

Die Tester verhielten sich wie reale Angreifer und nutzten für ihre Cyberattacken umfassende Angriffsketten. Als erstes sondierten sie die Ziele mithilfe verschiedener Tools, Techniken und Vektoren. Anschließend versuchten sie sich auf niedrigerer Ebene und mit größerer Wirksamkeit Zugang zu verschaffen. Im letzten Schritt ging es darum, Informationen zu stehlen, Systeme zu beschädigen und sich mit anderen Systemen innerhalb des Netzwerkes zu verbinden.

MANAGEMENT
Chief Executive Officer Simon Edwards
Chief Operations Officer Marc Briggs
Chief Human Resources Officer Magdalena Jurenko
Chief Technical Officer Stefan Dumitrascu

TESTTEAM
Nikki Albesa
Zaynab Bawa
Thomas Bean
Solandra Brewster
Rory Brown
Liam Fisher
Gia Gorbold
Jeremiah Morgan
Joseph Pike
Dave Togner
Dimitrios Tsarouchas
Stephen Withey
Liangyi Zhen

IT-UNTERSTÜTZUNG
Danny King-Smith
Chris Short

VERÖFFENTLICHUNG
Sara Claridge
Colin Mackleworth

Website selabs.uk
Twitter @SELabsUK
E-Mail info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog blog.selabs.uk
Telefon +44 (0)203 875 5000
Anschrift SE Labs Ltd,
55A High Street, Wimbledon, SW19 5BA, UK

SE Labs ist nach ISO/IEC 27001:2013 und BS EN ISO 9001:2015 für die Durchführung von IT-Sicherheitsprodukttests zertifiziert.

SE Labs ist Mitglied der Microsoft Virus Information Alliance (VIA), der Anti-Malware Testing Standards Organization (AMTSO) sowie der Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG).

Lizenziert zur Wiederveröffentlichung durch BlackBerry Limited

INHALT

Dokumentversion 1.0 erstellt am: 15. Juli 2021

EINLEITUNG

Präventiver Endpunktschutz

Wollen Sie nicht auch, dass Ihre Sicherheitslösung Unbefugte stoppt, bevor sie Ihre Systeme und Netzwerke kapern?

Es gibt viele Möglichkeiten, böswilligen Angreifern auf die Schliche zu kommen und sie aufzuhalten. Zahlreiche Produkte erkennen Phishing-Mails bereits beim Versand. Oder wenn E-Mails schädliche Links mit bösartigem Code enthalten. Einige Produkte laufen auf Hochtouren, wenn Malware ins System eindringt. Andere wiederum werden aktiv, wenn jemand im Netzwerk schlechtes Benehmen an den Tag legt.

Wann auch immer Ihre Sicherheitsmaßnahmen greifen, Sie möchten sicherlich, dass Angriffe aller Art erkannt und verhindert werden, bevor die Presse Wind von dem Geschehen erhält.

Unser Breach Response Test ist einzigartig, denn wir unterziehen die Produkte einem umfassenden und realistischen Härtetest. Wir replizieren aktuelle Angriffsketten und folgen der Kill Chain, um zu prüfen, wie die einzelnen Produkte die verschiedenen Bedrohungen erkennen und abwehren.

Sie wollen letztlich sicher sein, dass Ihr Sicherheitsprodukt das tut, was es soll: Vorfälle in irgendeiner Form zu verhindern. Es ist aber vernünftiger, eine Bedrohung im Keim zu ersticken, statt tatenlos zuzusehen und hinterher den entstandenen Schaden zu beseitigen.

Einige Produkte wurden ausschließlich für Beobachtungs- und Informationszwecke entwickelt. Andere hingegen können auch eingreifen und Bedrohungen aktiv beseitigen. Manche bereits beim ersten Anzeichen, andere erst nachdem der Schaden schon entstanden ist. Bei den „Beobachter-Produkten“ führen wir den Breach Response Test im Erkennungsmodus durch, bei „Stoppern“ wie **BlackBerry Protect** prüfen wir die Wirksamkeit im Schutzmodus.

In diesem Report untersuchen wir, wie **BlackBerry Protect** mit komplexen Angriffsversuchen in den einzelnen Phasen umgeht. Wann erkennt es Angriffe und wann schützt es? Ermöglicht es den gewohnten Geschäftsbetrieb und wie behandelt es legitime Anwendungen?

Es empfiehlt sich, die Fähigkeiten der einzelnen Sicherheitsprodukte zu kennen, bevor man sie in einem realen Szenario einsetzt. Mit den Breach Response Testberichten von SE Labs können Sie die Produkte finden, die am besten zu Ihren Anforderungen passen.

Wenn Sie einige Details in diesem Report nicht verstehen oder mit uns darüber sprechen möchten, kontaktieren Sie uns bitte über unsere Twitter- oder Facebook-Accounts. SE Labs verwendet Threat Intelligence, um die Tests so realistisch wie möglich durchzuführen. Wenn Sie wissen wollen, wie wir testen, was wir unter Threat Intelligence verstehen und wie wir diese zur Optimierung unserer Tests nutzen, besuchen Sie einfach unsere Website und folgen Sie uns auf Twitter.

Executive Summary

BlackBerry Protect und Optics wurden von uns intensiv getestet. Hierbei kamen dieselben Techniken zum Einsatz, die aktuell auch Cyberkriminelle nutzen, um Systeme zu kompromittieren und sich in Zielnetzwerke einzunisten.

Diese Fähigkeiten haben wir dabei genauer unter die Lupe genommen:

- Erkennung von zielgerichteten Angriffen
- Schutz vor den Folgen zielgerichteter Angriffe
- Behebung der Schäden und anderer Risiken, die aus diesen Bedrohungen folgen
- Umgang mit legitimen Anwendungen und anderen Objekten

Wir haben auch legitime Dateien verwendet, um die False-Positive-Rate zu messen und andere weniger optimale Interaktionen aufzudecken.

BlackBerry Protect und Optics ist bewundernswert. Die Lösungen bieten vollständige Erkennung und umfassenden Schutz. Zugleich ermöglichen sie die Ausführung aller legitimen Anwendungen. Dies ist ein außergewöhnliches Ergebnis in einem anspruchsvollen Test.

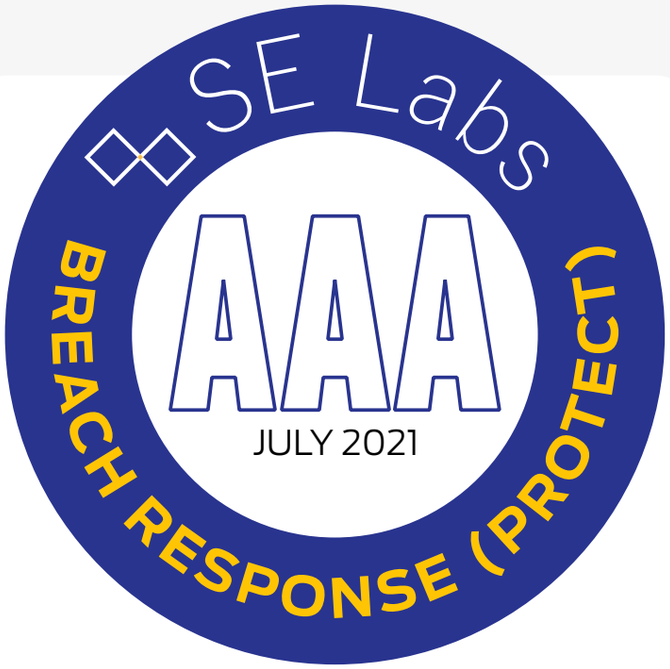
Fazit			
Getestetes Produkt	Genauigkeitsgrad beim Schutz (%)	Genauigkeit bei der Legitimität (%)	Gesamtgenauigkeit (%)
BlackBerry Protect und Optics	92 %	100 %	95 %

Grün zeigt an, dass das Produkt sehr genau ist und die Gesamtgenauigkeit bei ≥ 85 % liegt. Gelb entspricht einer mittleren Genauigkeit. Der Grad liegt zwischen 75 und 85 %. Rot weist auf eine geringe Genauigkeit hin. Sie beträgt weniger als 75 %.

SE Labs

Breach Response Award

Das folgende Produkt hat die SE Labs-Auszeichnung erhalten:



BlackBerry Protect und Optics

1. Testmethode und Testziel

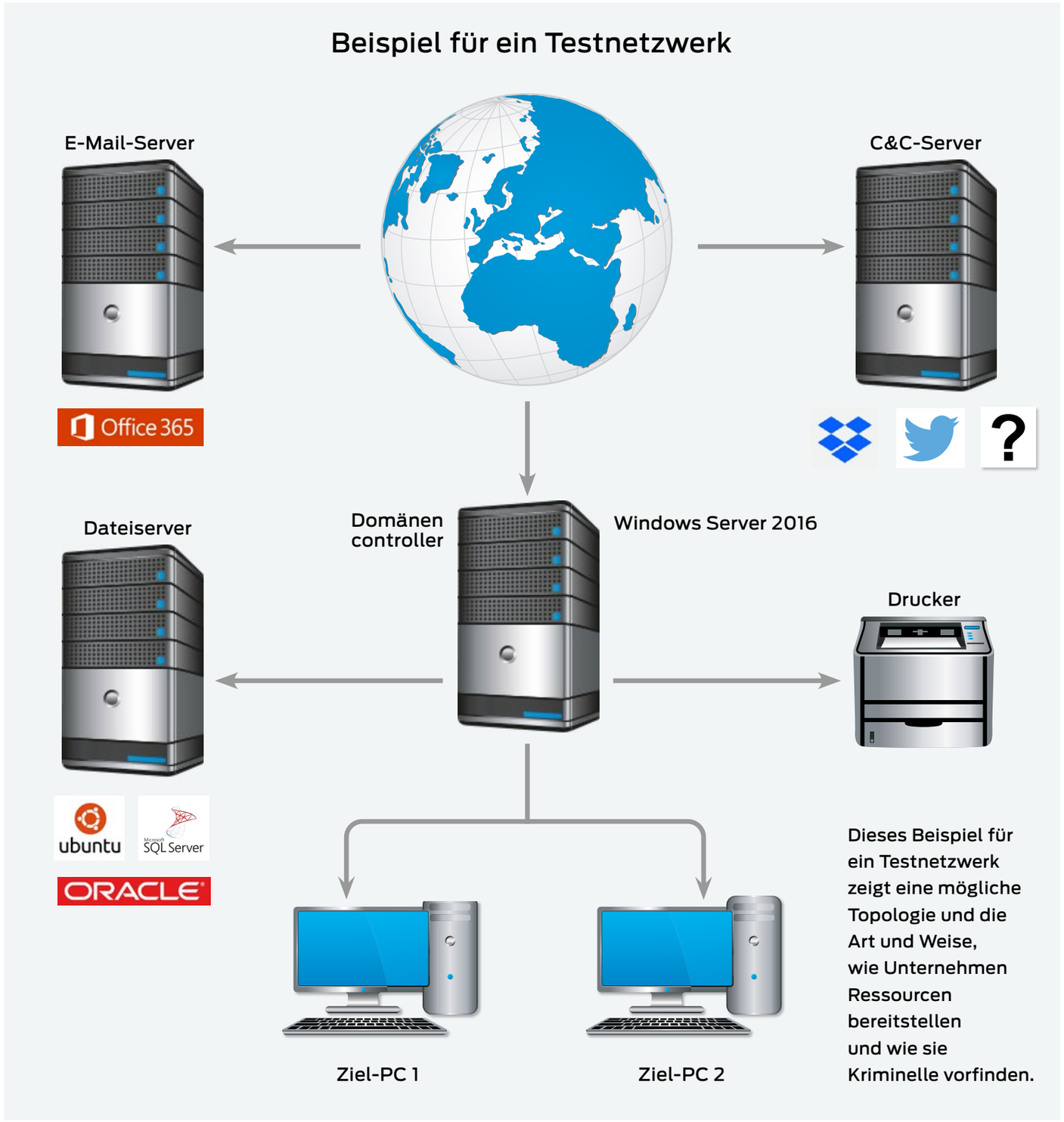
Tester können nicht davon ausgehen, dass die Produkte wie vom Anbieter beschrieben funktionieren. Für einen realistischen Breach Response Test wird ein echtes Netzwerk benötigt, das einem typischen Kundennetzwerk entspricht und so gehackt wird, wie reale Angreifer vorgehen würden.

Wie ein solches Netzwerk aufgebaut sein kann, zeigt Ihnen die Abbildung rechts. Zur Basis-Infrastruktur gehören Dateiserver, ein Domänencontroller sowie cloudbasierte E-Mails sowie ein bösartiger Command-and-Control-Server (C&C-Server), bei dem es sich um einen herkömmlichen Computer oder einen Dienst wie Dropbox, Twitter, Slack oder etwas anderes handeln kann.

Warum das alles nötig ist, können Sie **auf Seite 7** nachlesen. Denn Angreifer springen häufig von einem kompromittierten System zum anderen. Damit Sicherheitsprodukte dieses sogenannte „Lateral Movement“ auch erkennen können, muss die Nachbildung des Netzwerkes so realistisch wie möglich sein.
Es müssen Systeme vorhanden sein, die angreifbar sind und für die sich ein Angriff lohnt.

Da auch Unternehmensdrucker und andere IoT-Geräte kompromittiert werden können, haben wir stellvertretend für diese Geräte einen Drucker in die Abbildung aufgenommen.

Das Verhalten der Cyberkriminellen in der realen Welt entscheidet über die Angriffsmethode in unserem Test. Um in die Rolle der Angreifer schlüpfen zu können, beobachten wir ihre Taktiken und replizieren ihr Vorgehen. Mehr dazu finden Sie **auf den Seiten 9, 13 bis 16** und im **Anhang C.**



Reaktionen auf Bedrohungen

Vollständige Angriffskette: Alle Erkennungs- und Schutzmechanismen auf dem Prüfstand

Angreifer beginnen an einem bestimmten Punkt und machen so lange weiter, bis sie entweder ihr Ziel erreicht haben oder am Ende ihrer Möglichkeiten sind. Das kann eine Deadline sein oder die Grenze ihrer Fähigkeiten. Der Test muss dementsprechend auch an einem realistischen Ausgangspunkt mit einer typischen Aktion beginnen, beispielsweise mit dem Versenden einer Phishing-E-Mail oder dem Einrichten einer schädlichen Website. Auch die vielen kleinen Schritte, die nötig sind, um tatsächlich Daten zu kidnappen oder um Schaden im Netzwerk anzurichten, müssen gegangen werden.

Setzt der Test erst an einem späteren Punkt in der Angriffskette an, z. B. bei der Ausführung von Malware auf einem Endpunkt, gelingt es nicht, vollumfänglich die Erkennungs-, Schutz- und Abwehrfähigkeiten zu testen. Ist der Test abgeschlossen, bevor ein aussagekräftiger Schaden oder Diebstahl entstanden ist, kann das Produkt auch nicht seine Fähigkeiten bei der Verhaltenserkennung usw. beweisen.

Angriffsphasen

Die Abbildung unten zeigt den typischen Ablauf eines Angriffs. Der Test durchläuft jede Phase, da sich nur so die tatsächliche Wirksamkeit der Lösung ermitteln lässt. Unsere Testergebnisse zeigen die Erkennung und den Schutz in jeder dieser Phasen.

Wir messen die Reaktion des Produkts in den ersten Phasen des Angriffs, indem wir eine Bewertung der Erkennungs- und Schutzfähigkeiten vornehmen. Manche Produkte erkennen Bedrohungen, stoppen sie aber nicht. Andere lassen die Bedrohung kurz zu, bevor sie neutralisiert wird. Idealerweise erkennen und blockieren die Produkte die Bedrohungen, bevor sie ausgeführt werden. Diese Produkte eliminieren meist die Bedrohungen, stellen sie automatisch unter „Quarantäne“ oder speichern sie mit einem anderen sicheren Mechanismus für spätere Analysen.

Verläuft die erste Angriffsphase erfolgreich, prüfen wir die weitere Ausbreitung. Dies entspricht den Phasen 2–7, die wir folgendermaßen unterteilen: Zugriff (Phase 2), Aktion (Phase 3), Eskalation (Phase 4) und Post-Eskalation (Phase 5–7).

Abbildung 1 zeigt Ihnen einen typischen Angriff mit all seinen verschiedenen Phasen und Hacking-Aktivitäten. Dieser Ablauf entspricht einem „erfolgreichen“ Sicherheitsvorfall.

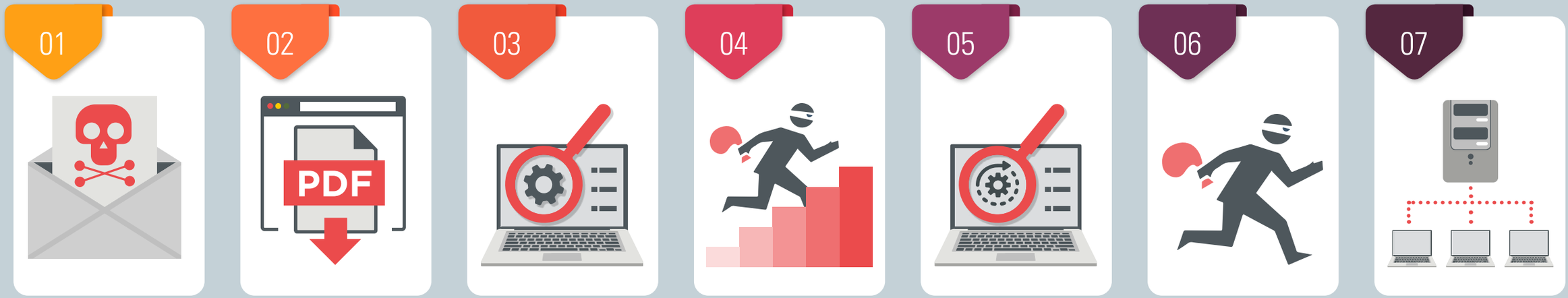


Abbildung 1: Ein Angriff beginnt in aller Regel mit einem Erstkontakt und durchläuft verschiedene Phasen, einschließlich Informationsbeschaffung, Datendiebstahl und Schadensausführung.

Abbildung 2 zeigt, dass der Angriff durch ein Produkt unterbrochen wurde und nur bis zu 3. Stufe vorgedrungen ist, wo er entdeckt und neutralisiert wurde. Der Angreifer konnte dementsprechend nicht die späteren Phasen durchlaufen.

Die Reihenfolge muss nicht bei jedem Angriff gleich sein. Ein Angreifer kann auch versuchen eine Verbindung zu anderen Systemen herzustellen, ohne dass er zuvor seine Rechte erweitern muss. Dennoch erfolgt häufig in der 5. Phase der Diebstahl von Passwörtern und Zugangsdaten, bevor der Angreifer seinen Marsch durch das Netzwerk fortsetzt.

Manche Angreifer richten zunächst einmal keinen Schaden an. Sie bevorzugen es, sich dauerhaft in den Systemen einzunisten, die Aktivitäten zu überwachen und nach und nach Informationen zu stehlen oder anderen subtileren Zielen nachzugehen.

In Abbildung 3 hat es der Angreifer geschafft bis zur fünften Stufe vorzudringen. Dies bedeutet: Das System wurde ernsthaft kompromittiert. Der Angreifer hat weitreichenden Zugang und ist im Besitz von Passwörtern. Seine Versuche, Daten aus dem Zielsystem abzuziehen, wurden ebenso geblockt wie seine Versuche, Schaden anzurichten.

ANGRIFFSKETTE: Wie Hacker vorgehen

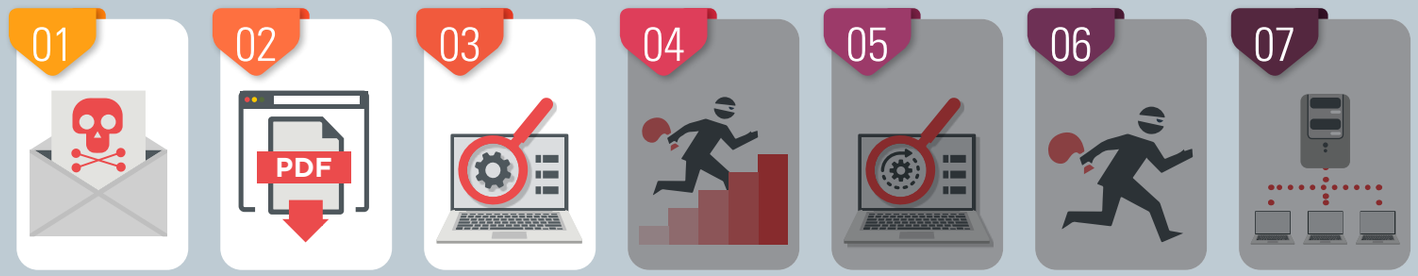


Abbildung 2: Dieser Angriff war anfänglich erfolgreich, konnte aber nur bis zur Phase der Informationsbeschaffung vordringen.

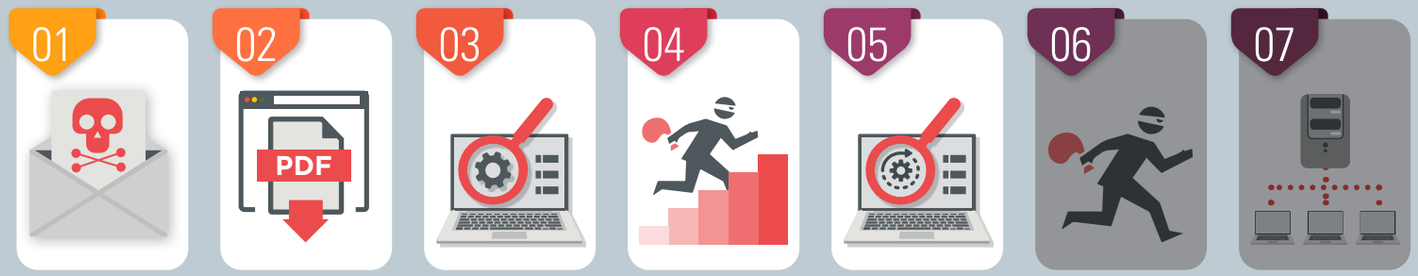


Abbildung 3: Dieser Angriff war erfolgreicher. Es gelang Passwörter abzugreifen, ein umfassender Diebstahl und eine Zerstörung wertvoller Daten wurden verhindert.

Angreifer und ihre Ziele

Wer die Verteidigung gegen gezielte Angriffe testet, muss sicherstellen, dass die Angriffe realistisch und relevant sind. Theoretisch kann jeder jeden angreifen. Gezielt oder nach dem Zufallsprinzip. Das müssen auch die Anbieter von Sicherheitslösungen beachten. Ihre Produkte müssen gängige Angriffsarten erkennen und verhindern können. Als Tester aber müssen wir Bedrohungen simulieren, die auch in der realen Welt vorkommen.

Sie sollten sich vor allen in diesem Test verwendeten Angriffen fürchten, denn sie können Ihrem Unternehmen ernsthaft schaden. Ohne Sicherheitsvorkehrungen käme es zu nachhaltigem Schaden: Ihre Systeme wären mit Ransomware infiziert, Unbefugte hätten Fernzugriff auf Ihr Netzwerk und Sie würden wertvolle Daten verlieren.

Allerdings haben wir nicht irgendwie getestet und uns Angriffsstrategien aus den Fingern gesaugt. Wir haben Threat Intelligence genutzt, um herauszufinden, welche fortgeschrittenen Bedrohungen kürzlich erfolgreich waren und haben das Vorgehen genau kopiert. Dadurch sind wir in der Lage, moderne Bedrohungen zu simulieren, die tagtäglich Regierungen auf der ganzen Welt, internationale Finanzinstitute und nationale Infrastrukturen gefährden.

Die Grafik rechts zeigt eine Übersicht von den Angriffsgruppen und ihren Zielen, die in diesem Test nachgeahmt wurden. Gelingt es einem Produkt diese Angriffe im Test zu erkennen und abzuwehren, ist die Wahrscheinlichkeit groß, dass es dies auch unter realen Bedingungen schafft. Besteht das Produkt diesen Test nicht, sollten Sie kühne Marketingaussagen mit Vorsicht genießen.

Mehr Informationen zu den einzelnen APT-Gruppen finden Sie **auf den Seiten 13–16**.

Angreifer und ihre Ziele

Angreifer/ APT-Gruppe	Methode	Ziel	Details
FIN7 und Carbanak			Dokumente mit versteckten Links zu Skripten
FIN4			Man-in-the-Middle-Spear-Phishing
FIN10			Spear-Phishing-E-Mails in Kombination mit öffentlichen Angriffstools
Silence			Dokumente, die Skripte, Links und Exploits enthalten

Hauptziele

2. Bewertung der Gesamtgenauigkeit

Es ist eine Kunst für sich, die Wirksamkeit einer Endpoint Security-Lösung zu bewerten. Viele Faktoren wirken sich auf die Performance aus und müssen deshalb berücksichtigt werden. Zum besseren Verständnis haben wir deshalb die verschiedenen Ergebnisse in einer Übersicht zusammengefasst.

In die Bewertung fließt neben den Erkennungs- und Schutzfähigkeiten des Produkts auch der Umgang mit nicht bösartigen Objekten wie Webadressen (URLs) und Anwendungen ein.

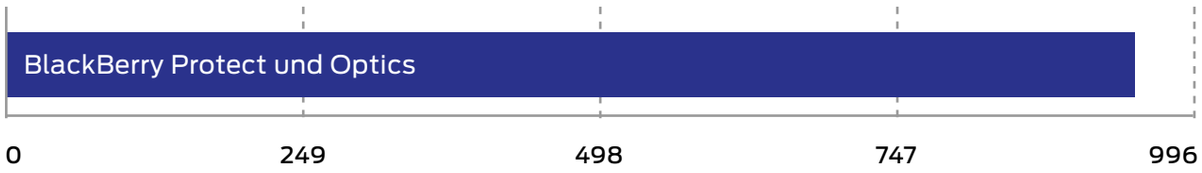
Die Fähigkeiten der einzelnen Produkte unterscheiden sich mitunter erheblich. Ein Produkt kann beispielsweise eine URL vollständig blockieren und dadurch die Bedrohung stoppen, wodurch weitere bösartige Ereignisse unterbleiben. Ein anderes Produkt lässt möglicherweise die Ausführung webbasierter Exploits zu, verhindert aber das Herunterladen von weiterem Code. Wieder andere lassen es zu, dass Malware kurzzeitig ausgeführt wird, bevor das schädliche Verhalten erkannt und der Code gelöscht wird. Oder zur späteren Analyse unter „Quarantäne“ gestellt wird. All dies fließt in die endgültige Bewertung ein.

Ein Produkt, das die Bedrohungen vollständig blockiert, wird höher bewertet als eines, das die Ausführung erst zulässt und dann die Folgen beseitigt. Produkte, die viele Malware-Infektionen zulassen und legitime Anwendungen blockieren, werden dementsprechend schlechter bewertet.

Die Bewertung von Endpoint Security-Lösungen erfordert eine differenzierte Methode, die wir .

Bewertungen der Gesamtgenauigkeit

Produkt	Genauigkeitswert	Genauigkeitsgrad (%)	Auszeichnung
BlackBerry Protect und Optics	946	95 %	AAA



In die Bewertung fließen die Schutzfähigkeiten und False Positives ein.

3. Bewertungskriterien

Wir setzen die Sicherheitsprodukte in diesem Test Angriffen aus, die in mehreren Phasen ablaufen. Das perfekte Produkt erkennt und schützt vor allen relevanten Elementen der Angriffe. Der Begriff „relevant“ bedeutet hier, dass spätere Phasen nicht mehr betrachtet werden müssen, da sämtliche Attacken zuvor abgewehrt wurden.

In jedem Testfall kann das Produkt maximal 4 Punkte erreichen. Und zwar für die erfolgreiche Erkennung des Angriffs und den Schutz des Systems. Verhält sich das Produkt nicht wie gewünscht, werden maximal 9 Punkte abgezogen. Im schlechtesten Fall erhält ein Produkt also die Bewertung -5. Es gilt: Je schwerwiegender die Auswirkungen des Angriffs sind, desto höher die Abzüge. Folgende Kriterien fließen in die Bewertung ein:

Detection (–0,5)
Erkennt das Produkt eine Bedrohung nicht mit einem gewissen Grad an nützlichen Informationen, werden 0,5 Punkte abgezogen.

Execution (–0,5)
Auch das Ausführen einer Bedrohung hat einen Abzug von 0,5 Punkten zur Folge.

Action (–1)
Kann ein Angriff eine oder mehrere Aktionen ausführen oder das Ziel fernsteuern, wird 1 weiterer Punkt abgezogen.

Privilege Escalation (–2)
Kann ein Angreifer die Systemprivilegien ausweiten, werden zusätzlich 2 Punkte abgezogen.

Post Escalation Action (–1)
Lässt das Produkt neue, leistungsfähigere und heimtückischere Aktionen mit erweiterten Rechten zu, wird 1 weiterer Punkt abgezogen.

Lateral Movement (–2)
Kann der Angreifer das Ziel als Einstiegssystem in andere anfällige Systeme nutzen, werden 2 Punkte abgezogen.

Lateral Action (–2)
Weitere 2 Punkte Abzug gibt es, wenn der Angreifer auf dem neuen Ziel Aktionen durchführen und seinen Einfluss auf das Netzwerk ausweiten kann.

Um die Schutzbewertung zu berechnen, werden alle ermittelten Werte mit 4 multipliziert. Die von uns verwendete Gewichtung können Sie für eigene Bewertungen an Ihr persönliches Risikoprofil und verschiedenen Schutzniveaus anpassen. Wenn Sie die Höhe der Abzüge und den Gesamtschutz individuell gewichten, können Sie ganz einfach Ihr eigenes Bewertungssystem generieren.

Die Gesamtschutzbewertung ergibt sich wie folgt: Anzahl der geschützten Fälle multipliziert mit 4 (Standardhöchstpunktzahl) und reduziert um alle Abzüge. Das Ergebnis wird dann erneut mit 4 multipliziert (dem Gewichtungswert für Schutzbewertungen).

Response Details

Attacker/ APT Group	Number of test cases	Detection	Delivery	Execution	Action	Privilege Escalation	Post Escalation Action	Lateral Movement	Lateral Action	Protected	Penalties
FIN7 und Carbanak	13	13	0	13	0	0	0	0	0	13	10
FIN4	12	12	0	12	0	0	0	0	0	12	2
FIN10	9	9	0	9	0	0	0	0	0	9	7
Silence	6	6	0	6	0	0	0	0	0	6	6
Grand Total	**40**	**40**	**0**	**40**	**0**	**0**	**0**	**0**	**0**	**40**	**25**

Die Tabelle zeigt das Ergebnis des Produkts für die einzelnen Angriffsphasen jeder APT-Gruppe. Die Spalten „Delivery“ bis „Lateral Action“ zeigen, wie oft ein Angreifer diese Ziele erreichen konnte. Das ideale Ergebnis ist „0“.

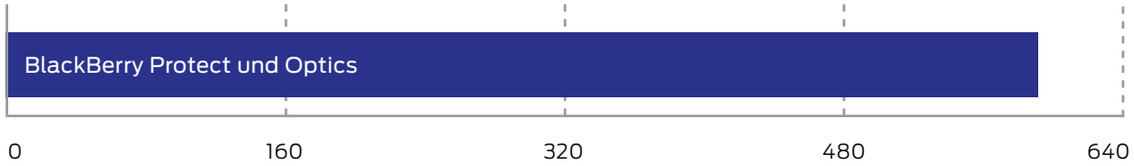
Protection Accuracy Rating Details

Attacker/ APT Group	Number of test cases	Protected	Penalties	Protection Score	Protection Rating
FIN7 und Carbanak	13	13	10	47	188
FIN4	12	12	2	47	188
FIN10	9	9	7	32.5	130
Silence	6	6	6	21	84
Grand Total	**40**	**40**	**25**	**147.5**	**590**

Zur Berechnung der Schutzbewertung werden verschiedene Schutzniveaus bzw. das Versagen des Schutzes herangezogen.

Protection Accuracy Ratings

Produkt	Protection Accuracy Rating	Protection Accuracy Rating (%)
BlackBerry Protect und Optics	590	92 %



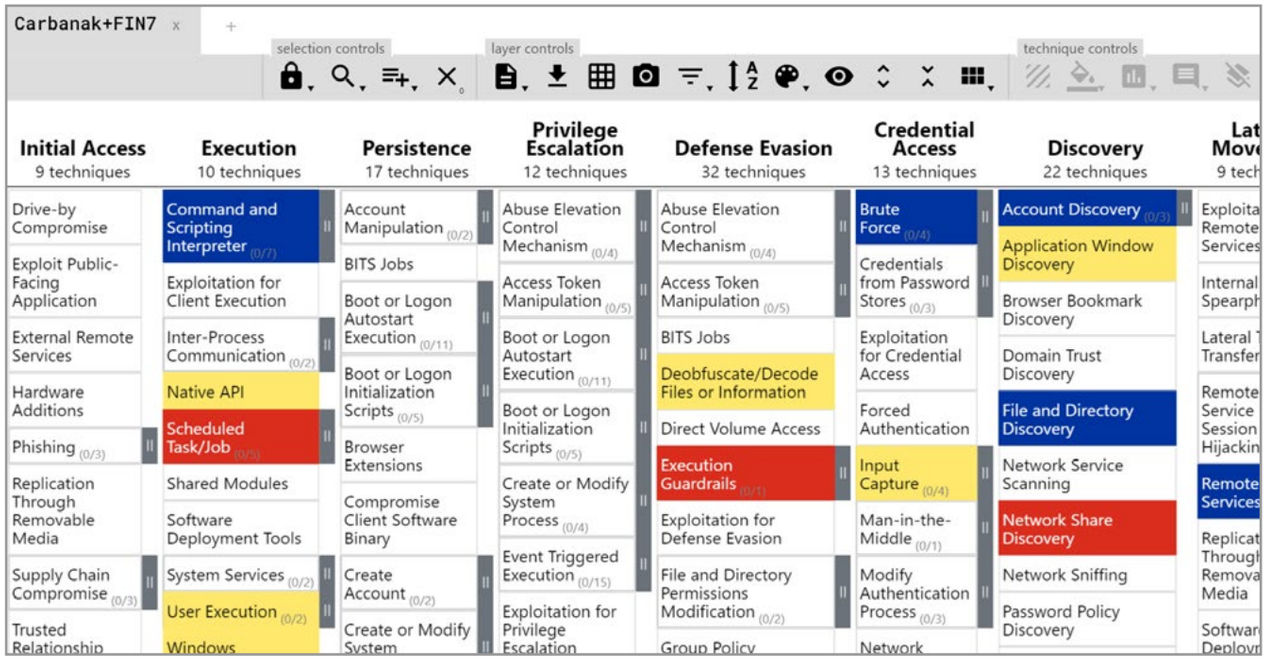
Der Umgang von Produkten mit Bedrohungen ist mehr als „gewinnen“ oder „verlieren“. Daher werden die Schutzbewertungen gewichtet.

4. Threat Intelligence

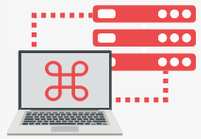
FIN7

Diese Angreifergruppe hat mit ihren Spear-Phishing-Attacken vor allem den Einzelhandel, die Gastronomie und das Gaststättengewerbe in den USA im Visier. Die Angriffe verbergen sich in Word- und RTF-Dokumenten hinter Kundenbeschwerden, Bewerbungen und Essensbestellungen. In Wirklichkeit handelt es sich um Angriffe mit bösartigem (VBS-)Code in versteckten Links.

Referenzen:
https://attack.mitre.org/groups/G0046/



Im MITRE ATT&CK-Framework dokumentierte Angreifertechnik

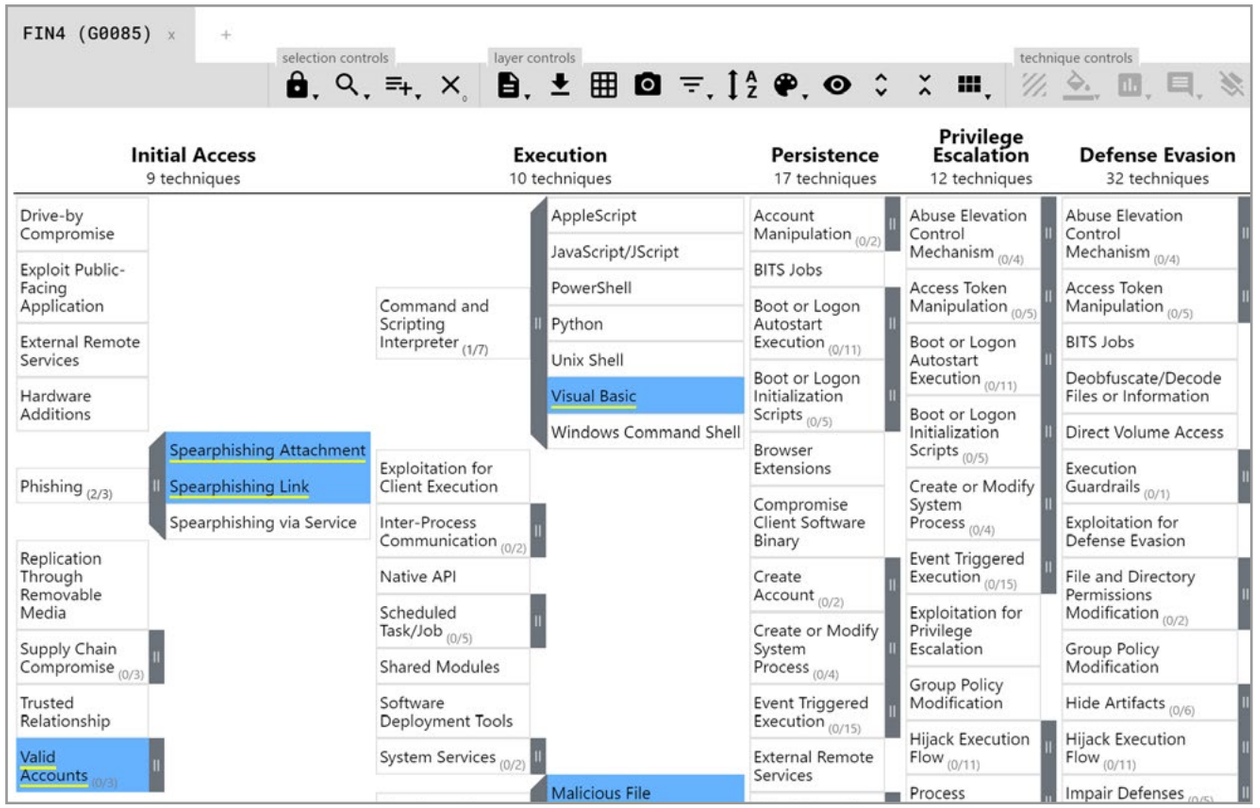
Example FIN7 Attack										
Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Bypass UAC	Code Signing	Brute Force	File and Directory Discovery	Remote Desktop Protocol	Data from Local System	Commonly Used Port	Data Compressed
	Service Execution	Valid Accounts		Disabling Security Tools	Credentials from Web Browsers	Process Discovery		Data Staged	Standard Non-Application Layer Protocol	Data Encrypted
	User Execution			Masquerading		System Information Discovery		Screen Capture	Remote Access Tools	Exfiltration over Command and Control Channel
				Process Injection		Query Registry				
						Permission Groups Discovery				
						System Network Configuration Discovery				
 E-mail Link - Fileless Attack	 Service Execution	 Valid Accounts	 Bypass UAC	 Disabling Security Tools	 Credentials from Web Browsers	 System Information Discovery	 Remote Desktop Protocol	 Screen Capture	 Remote Access Tools	 Exfiltration over Command and Control Channel

FIN4

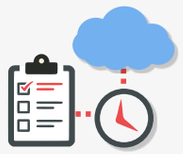
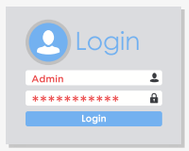
Diese Angreifergruppe stiehlt echte Office-Dokumente der Zielpersonen, überarbeitet sie und infiziert sie mit bösartigen Makros.

Die Verwendung korrekt formatierter Dokumente und echter Informationen erhöht die Wahrscheinlichkeit, dass die Opfer die kompromittierten Anhänge öffnen und dadurch zulassen, dass ihre eigenen Systeme kompromittiert werden.

Referenzen:
https://attack.mitre.org/groups/G0085/



Im MITRE ATT&CK-Framework dokumentierte Angreifertechnik.

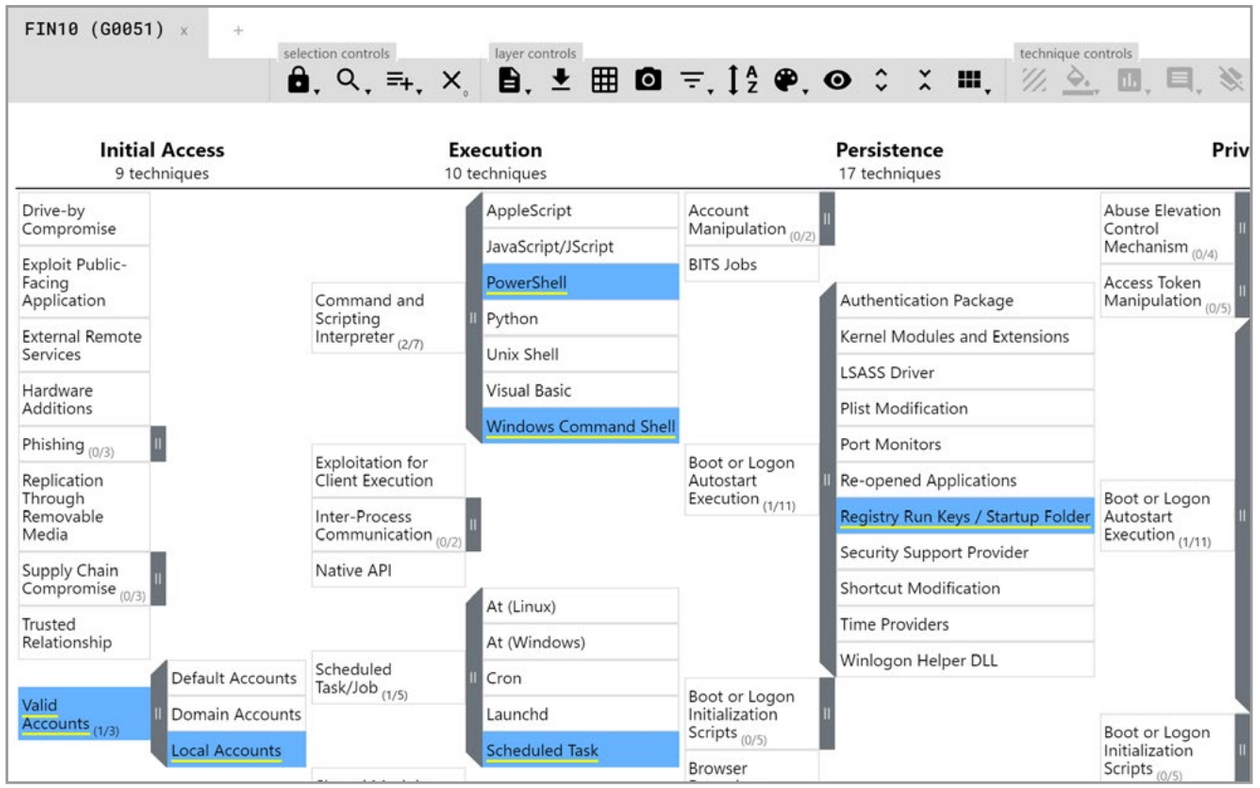
Example FIN4 Attack										
Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
Spearphishing Link	Scheduled Task	Scheduled Task	Valid Accounts	Software Packing	Input Capture	Account Discovery	Pass the Hash	Image Capture	Uncommonly used Port	Data Compressed
	User Execution				Input Prompt	File and Directory Discovery			Data Encoding	Data Encrypted
						Process Discovery				Exfiltration Over Command and Control Channel
 **E-mail Link - Fileless Attack**	 **User Execution**	 **Scheduled Task**	 **Valid Accounts**	 **Software Packing**	 **Input Prompt**	 **System Information Discovery**	 **Pass the Hash**	 **Image Capture**	 **Data Encoding**	 **Data Encrypted**

FIN10

Diese Angreifergruppe verwendet öffentlich bekannte Tools und Techniken, um in Kanada ansässige Kasinos und Rohstoffunternehmen zu kompromittieren. Sie droht ihren Opfern damit, die gestohlenen Daten zu veröffentlichen, um Geld zu erpressen.

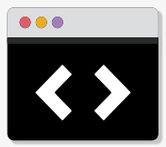
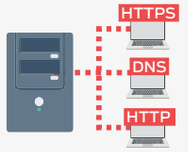
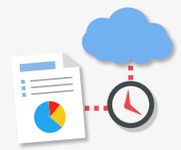
Für ihre Angriffe kombiniert die Gruppe Spear-Phishing-E-Mails mit Metasploit, PowerShell-Skripten und dem Online-Zugriffstool ReSplinterRat.

Referenzen:
https://attack.mitre.org/groups/G0051/



Im MITRE ATT&CK-Framework dokumentierte Angreifertechnik.

Example FIN10 Attack

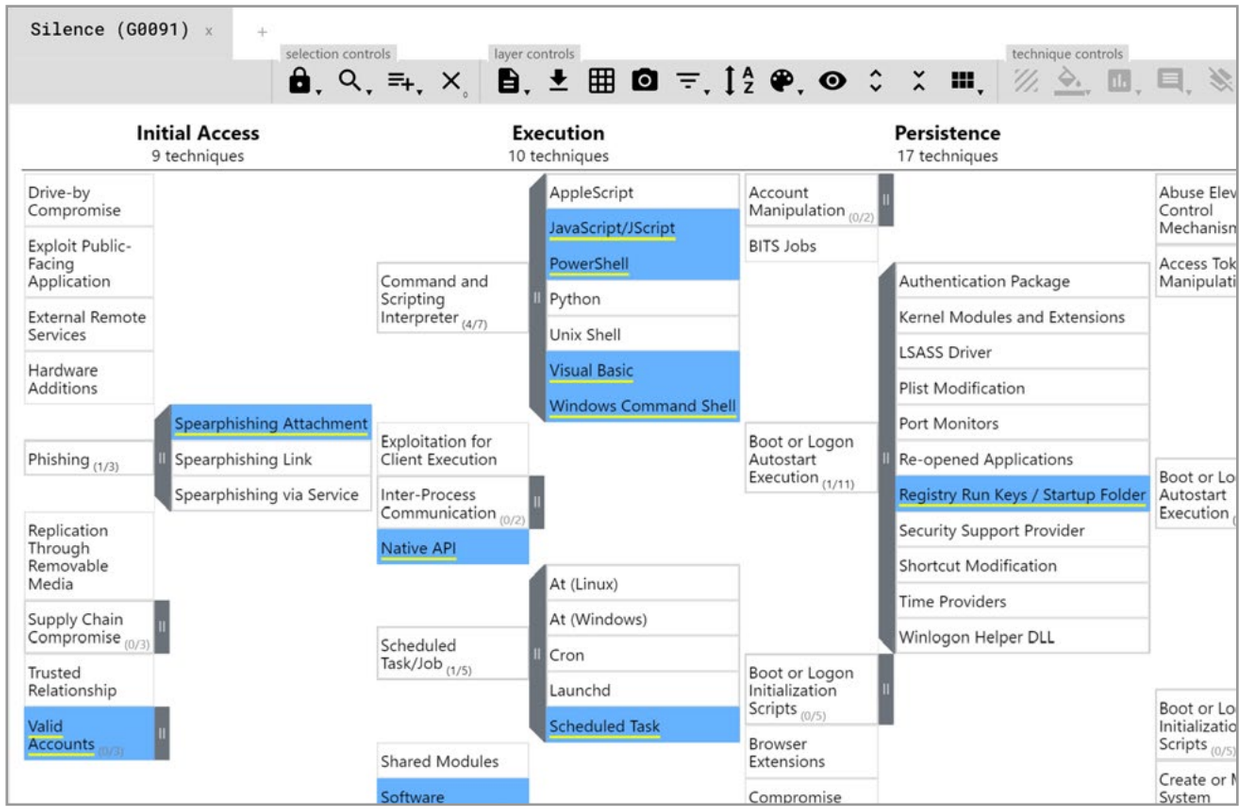
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Link	mshta Scripting User Execution	Registry Ru Key / Start Folder	Scheduled Tasks Valid Accounts	Scripting	No credential access seen in research for FIN10.	Account Discovery File and Directory Discovery Process Discovery System Information Discovery System Owner/User Discovery	Remote Desktop Protocol	Automated Collection	Commonly Used Port	Scheduled Transfer
 E-mail Link - Fileless Attack	 mshta	 Registry Ru Key/ Start Folder	 Valid Accounts	 Scripting		 Process Discovery	 Remote Desktop Protocol	 Automated Collection	 Commonly Used Port	 Scheduled Transfer

Silence

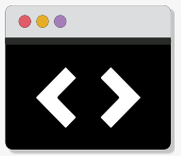
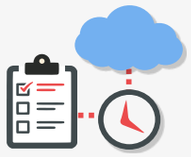
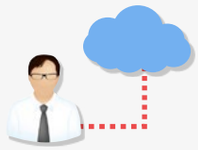
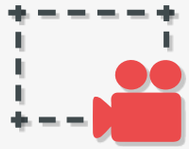
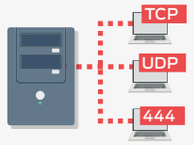
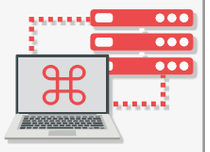
Diese Angreifergruppe konzentriert sich auf skriptbasierte Angriffe unter Verwendung von . CHM- und LNK-Dateien sowie Makros und anderen Exploits. Mit ihren kompromittierten Microsoft Office-Dokumenten nimmt sie sich Banken vor.

Diese Gruppe visiert Ziele auf der ganzen Welt an, doch in osteuropäischen Ländern ist sie besonders aktiv. Ihre spezifischen Ziele sind Geldautomaten.

Referenzen:
https://attack.mitre.org/groups/G0091/



Im MITRE ATT&CK-Framework dokumentierte Angreifertechnik.

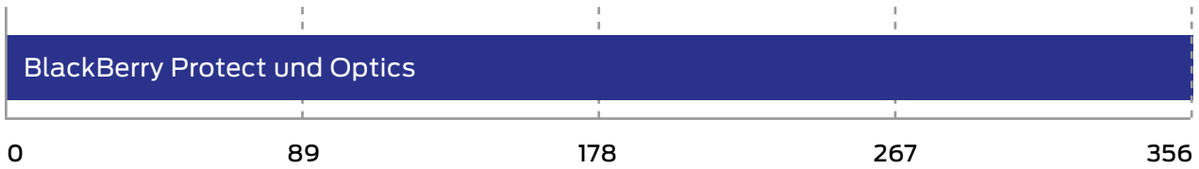
Example Silence Attack										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Attachment	Scripting	Scheduled Task	Scheduled Task	File Deletion	No Credential Access techniques seen in research for Silence.	Network Share Discovery	Windows Admin Shares	Video Capture	Uncommonly Used Port	Exfiltration Over Command and Control Channel
	Service Execution			Obfuscated Files or Information		Remote Share Discovery				
	User Execution			Scripting						
 E-mail Link - Fileless Attack	 Scripting	 Scheduled Task	 Scheduled Task	 File Deletion		 Network Share Discovery	 Windows Admin Shares	 Video Capture	 Uncommonly Used Port	 Exfiltration Over Command and Control Channel

5. Bewertung legitimer Software

Diese Bewertungen zeigen, wie exakt das Produkt legitime Anwendungen und URLs einstuft. Dabei geht es auch um die Interaktion mit dem Anwender. Im Idealfall stuft ein Produkt legitime Objekte nicht oder als sicher ein. Und das, ohne den Anwender in irgendeiner Form zu stören.

Bei diesem Test berücksichtigen wir auch die Verbreitung (Beliebtheit) der Anwendungen und Websites. Stuft ein Produkt sehr beliebte Software und Websites falsch ein, gibt es höhere Abzüge.

Bewertungen legitimer Software		
Produkt	Legitimer Genauigkeitsgrad	Legitime Genauigkeit (%)
BlackBerry Protect und Optics	356	100 %



Bewertungen legitimer Software geben an, wie gut die Detection Engine eines Anbieters funktioniert.

6. Fazit

Dieser Test umfasste die größte Bandbreite an Bedrohungen, die es bis dato in einem öffentlich verfügbaren Test gab. **BlackBerry Protect und Optics** wurden einer Vielzahl von Exploits, dateilosen Angriffen und Malware-Anhängen ausgesetzt.

Alle diese Angriffsarten waren in den letzten Jahren auch an realen Angriffen beteiligt. Sie sind repräsentativ und stellen realistische Bedrohungen von Unternehmensnetzwerken auf der ganzen Welt dar. Sie sind praktisch oder tatsächlich deckungsgleich mit auf den Seiten 9 und **13 bis 16** dargestellten Bedrohungen oder Bedrohungsgruppen.

Wir möchten betonen, dass bei diesem Test zwar dieselben Angriffsarten, aber neue Dateien zum Einsatz kamen. Denn nur so konnte getestet werden, ob das Produkt auch bestimmte Angriffsmethoden auf Systeme erkennt und davor schützt. Sonst wäre es nur ein Test zur Erkennung bösartiger Dateien gewesen, die in den letzten Jahren bekannt geworden sind. Die Ergebnisse sind also ein Indikator für die potenzielle künftige Leistung des Produkts.

Das Produkt erkannte alle Bedrohungen und bot vollständigen Schutz. In allen getesteten Fällen kamen die Bedrohungen nicht über die ersten Stufen der Angriffskette hinaus. War ein Zielsystem einer Bedrohung ausgesetzt, wurde diese sofort erkannt und an der Ausführung gehindert. Dadurch wurde größerer Schaden verhindert und ein Datendiebstahl abgewendet.

Kein einziger Angriff kam so weit, dass die Tester mit dem Hacken der Systeme beginnen konnten. Manche Produkte reagieren an dieser Stelle zu aggressiv und können nicht zwischen Bedrohungen und legitimen Objekten unterscheiden. **BlackBerry Protect und Optics** hat in diesem Test keine False Positives erzeugt. Für die überzeugenden Ergebnisse und seine hervorragende Leistung erhält **BlackBerry Protect und Optics** eine **AAA**-Auszeichnung.

Anhänge

ANHANG A: Glossar

BEGRIFF	BEDEUTUNG
Compromised	Der Angriff war erfolgreich und die Schadsoftware konnte ungehindert auf dem Zielsystem ausgeführt werden. Der Angreifer war in der Lage, das System per Fernsteuerung zu übernehmen und eine Vielzahl von Aufgaben auszuführen.
Blocked	Der Angriff wurde verhindert. Änderungen am Ziel waren nicht möglich.
False Positive	Ein „False Positive“ liegt vor, wenn ein Sicherheitsprodukt eine legitime Anwendung oder Website fälschlicherweise als bösartig einstuft.
Neutralised	Der Exploit oder die Malware-Nutzlast lief kurz auf dem Ziel, wurde aber später entfernt.
Complete Remediation	Das Sicherheitsprodukt hat alle nennenswerten Spuren eines Angriffs beseitigt.
Ziel	Hier ist es das Testsystem, das durch ein Sicherheitsprodukt geschützt wird.
Threat	Ein Programm oder eine Abfolge von Interaktionen mit dem Zielsystem, um es im gewissen Umfang unberechtigt kontrollieren zu können.
Update	Hersteller von Sicherheitsprodukten aktualisieren ihre Produkte regelmäßig, um mit den neuesten Bedrohungen Schritt zu halten. Updates können als Datei(en) heruntergeladen oder via Internet angefordert werden.

ANHANG B: FAQ

Eine vollständige Methodik für diesen Test finden Sie auf unserer Website.

- Der Test fand zwischen dem 7. April und dem 11. Mai 2021.
- Das Produkt wurde nach den Empfehlungen des Herstellers konfiguriert.
- Die gezielten Angriffe wurden von SE Labs ausgewählt und überprüft.
- Die bösartigen und legitimen Daten wurden den Partnerorganisationen nach Abschluss des Tests zur Verfügung gestellt.
- SE Labs führte diesen Test zur Sicherheit von Endpunkten auf physischen PCs durch, nicht auf virtuellen Maschinen.

Q Was ist eine Partnerorganisation? Erhalte ich als Partner Zugriff auf die in Ihren Tests verwendeten Bedrohungsdaten?

A Partnerorganisationen profitieren von unseren Beratungsservices, nachdem ein Test durchgeführt wurde. Sie erhalten Zugriff auf einen kleinen Teil der Daten, damit sie ihre Produkte verbessern können. Und sie können Logos mit der Auszeichnung für Marketingzwecke verwenden. Daten des Partners geben wir nicht an andere Partner weiter. Partner kann nur werden, wer sich an unseren Tests beteiligt.

Q Wir überlegen, ob wir ein Endpoint Protection und/oder Endpoint Detection and Response (EDR) Produkt kaufen oder austauschen. Können Sie uns dabei helfen?

A Ja. Wir führen häufig vertrauliche Tests für Unternehmen durch, die über einen Wechsel ihrer Sicherheitsprodukte nachdenken. Kontaktieren Sie uns einfach unter info@selabs.uk für nähere Informationen.

ANHANG C : Angriffsdetails

FIN7											
Incident No:	**Initial Access**	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
1	Spearphishing Attachment	Command-Line Interface	New Service	Bypass UAC	Obfuscated Files or Information	Credential Dumping	Account Discovery	Remote File Copy	Data from Local System	Commonly Used Port	Data Compressed
		Powershell	Scheduled Task	Valid Accounts	Modify Registry	Input Capture	File and Directory Discovery	Pass the Hash	Data Staged	Standard Application Layer Protocol	Data Encrypted
		Scripting			File Deletion		Process Discovery		Input Capture	Standard Cryptographic Protocol	Exfiltration over Command and Control Channel
		Remote File Copy			Process Hollowing		Query Registry				
		User Execution			Virtulisation/ Sandbox Evasion		System Information Discovery				
							System Owner/User Discovery				
2	Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Bypass UAC	Code Signing	Brute Force	File and Directory Discovery	Remote Desktop Protocol	Data from Local System	Commonly Used Port	Data Compressed
		Service Execution	Valid Accounts		Disabling Security Tools	Credentials from Web Browsers	Process Discovery		Data Staged	Standard Non-Application Layer Protocol	Data Encrypted
		User Execution			Masquerading		System Information Discovery		Screen Capture	Remote Access Tools	Exfiltration over Command and Control Channel
					Process Injection		Query Registry				
							Permission Groups Discovery				
							System Network Configuration Discovery				
3	Spearphishing Attachment	Command-Line Interface	Application Shimming	Bypass UAC	Deobfuscate Files or Information	Brute Force	File and Directory Discovery	Remote File Copy	Data from Local System	Commonly Used Port	Data Compressed
		mshta			Execution Guardrails	Credential Dumping	Process Discovery	Pass the Hash	Data Staged	Connection Proxy	Data Encrypted
		User Execution			Software Packing		System Information Discovery	Windows Admin Shares		Standard Non-Application Layer Protocol	Exfiltration over Command and Control Channel
		Scripting					Network Share Discovery				
							System Network Configuration Discovery				
							System Owner/User Discovery				
							Account Discovery				

FIN7

Incident No:	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
4	Spearphishing Attachment	Command-Line Interface	Hooking	DLL Search Order Hijacking	Indirect Command Execution [NEW]	Hooking	File and Directory Discovery	Windows Management Instrumentation [NEW]	Data from Local System	Commonly Used Port	Data Compressed
		Powershell			File Deletion	Input Capture	Process Discovery		Data Staged	Standard Application Layer Protocol	Data Encrypted
		Scripting			Execution Guardrails		System Information Discovery			Standard Cryptographic Protocol	Exfiltration over Command and Control Channel
		Component Object Model and Distributed COM					Application Windows Discovery				
		Execution through API					Permission Groups Discovery				
							Network Share Discovery				

FIN4

Incident No:	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
5	Spearphishing Attachment	Scripting	New Service	Valid Accounts	Scripting	Input Capture	Account Discovery	Remote Desktop Protocol	Email Collection	Commonly Used Port	Automated Exfiltration
		User Execution				Input Prompt	File and Directory Discovery			Standard Application Layer Protocol	Exfiltration Over Alternative Protocol
							Process Discovery				Data Transfer Size Limits
							System Information Discovery				
6	Spearphishing Link	Scheduled Task	Scheduled Task	Valid Accounts	Software Packing	Input Capture	Account Discovery	Pass the Hash	Image Capture	Uncommonly used Port	Data Compressed
		User Execution				Input Prompt	File and Directory Discovery			Data Encoding	Data Encrypted
							Process Discovery				Exfiltration Over Command and Control Channel
							System Information Discovery				
7	Spearphishing Attachment	Regsvcs/Regasm	New Service	Valid Accounts	Process Injection	Input Capture	Account Discovery	Remote File Copy	Image Capture	Standard Application Layer Protocol	Scheduled Transfer
		User Execution				Input Prompt	File and Directory Discovery			Process Injection	Exfiltration Over Alternative Protocol
							Process Discovery			Commonly Used Port	
							System Information Discovery				
8	Spearphishing Link	Scripting	Start Up Items	Valid Accounts	Scripting	Input Capture		Remote File Copy	Email Collection	Uncommonly used Port	Data Compressed
		User Execution				Input Prompt				Web Service	Data Encrypted
											Exfiltration Command and Control Channel

FIN10											
Incident No:	**Initial Access**	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
9	Spearphishing Attachment	User Execution	Scheduled Tasks	Scheduled Tasks Valid Accounts	File Deletion	No credential access seen in research for FIN10.	Account Discovery File and Directory Discovery Process Discovery System Information Discovery System Owner/User Discovery	Remote File Copy	Data from Local System Data Staged	Commonly Used Port	Exfiltration Over Command and Control Channel
10	Spearphishing Link	mshta Scripting User Execution	Registry Ru Key / Start Folder	Scheduled Tasks Valid Accounts	Scripting	No credential access seen in research for FIN10.	Account Discovery File and Directory Discovery Process Discovery System Information Discovery System Owner/User Discovery	Remote Desktop Protocol	Automated Collection	Commonly Used Port	Scheduled Transfer
11	Spearphishing Link	Powershell Scripting Regsvcs/Regasm User Execution	Scheduled Tasks	Scheduled Tasks Valid Accounts	Regsvcs/Regasm Scripting	No credential access seen in research for FIN10.	Account Discovery File and Directory Discovery Process Discovery System Information Discovery System Owner/User Discovery	Remote File Copy	Automated Collection	Commonly Used Port	Scheduled Transfer

Silence											
Incident No:	**Initial Access**	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
12	Spearphishing Attachment	Command-Line Interface Compiled HTML File Execution through API User Execution	Scheduled Task	Scheduled Task	Compiled HTML File File Deletion	No Credential Access techniques seen in research for Silence.	Network Share Discovery Remote Share Discovery	Windows Admin Shares	Screen Capture	Commonly Used Port	Exfiltration Over Command and Control Channel
13	Spearphishing Attachment	Scripting Service Execution User Execution	Scheduled Task	Scheduled Task	File Deletion Obfuscated Files or Information Scripting	No Credential Access techniques seen in research for Silence.	Network Share Discovery Remote Share Discovery	Windows Admin Shares	Video Capture	Uncommonly Used Port	Exfiltration Over Command and Control Channel

SE Labs

SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising his report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an “AS IS” basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.