Ein Rückblick auf sechs Monate Ukraine-Krieg: Welche Strategie verfolgten die russischen Cyberangriffe und wie wirkungsvoll waren sie bisher?

Chester Wisniewski, Principal Research Scientist bei Sophos beschreibt das russische Cyber-Vorgehen im Vorfeld und während des Ukrainekriegs anhand von vier Kategorien: Zerstörung, Desinformation, Hacktivismus und E-Spionage
Von Chester Wisniewski, Principal Research Scientist bei Sophos

Als Russland am 24. Februar 2022 in die Ukraine einmarschierte, wusste trotz vieler Einschätzungsversuche niemand von uns, welche Rolle Cyberangriffe bei einer umfassenden Invasion spielen könnten. Russland hatte seit der Besetzung der Krim im Jahr 2014 Cyberangriffe auf die Ukraine durchgeführt, und es schien unvermeidlich, dass diese Tools weiterhin eine Rolle spielen würden, insbesondere nach den Angriffen auf das ukrainische Stromnetz und der weltweiten Verbreitung des NotPetya-Wurms.

Eine der Herausforderungen bei der Bewertung der Wirksamkeit oder Auswirkung von Cyberangriffen besteht darin, zu sehen, wie sie in das „große Ganze" passen. Wenn wir uns mitten in einem Konflikt befinden, verschleiert und verzerrt der „Informationsnebel" des Krieges oft unsere Sicht auf die Wirksamkeit einer bestimmten Aktion. Lassen Sie uns jetzt, mehr als sechs Monate nach Kriegsbeginn, zurückblicken und versuchen, die Rolle von Cyberwaffen bis zu diesem Zeitpunkt zu bestimmen.

Nach Angaben des Ukrainischen Staatsdienstes für besonderen Kommunikations- und Informationsschutz (SSSCIP) wurde die Ukraine seit Beginn des Krieges 1.123 Mal angegriffen. 36,9 % der Ziele betrafen die Regierung/Verteidigung und die Angriffe bestanden zu 23,7 % aus bösartigem Code und zu 27,2 % aus dem Sammeln von Informationen.

Die Cyber-Komponente des Krieges begann fast 24 Stunden vor der Landinvasion. In meinem Tagebuch über den Konflikt notierte ich, dass DDoS-Angriffe und Wiper-Angriffe am 23. Februar gegen 16:00 Uhr Ortszeit begannen. Unmittelbar danach wurde es sehr unübersichtlich, da eine Vielzahl von Angriffen und Techniken parallel zum Einsatz kamen. Zur besseren Analyse von Intensität, Wirksamkeit und Zielen habe ich diese Attacken in die vier Kategorien Zerstörung, Desinformation, Hacktivismus und Spionage unterteilt.

Strategie 1: Zerstörung
Da sich der Krieg für Russland nicht nach Plan entwickelte, wurden einige dieser Techniken bisher in verschiedenen Phasen des Krieges unterschiedlich eingesetzt. Die erste und offensichtlichste war die destruktive Malware-Phase. Ab Januar 2022 begannen laut SSSCIP russische und pro-russische Angreifer, Wiper- und Bootsektor-verändernde Malware freizusetzen, die darauf abzielte, den Inhalt eines Systems zu löschen oder es funktionsunfähig zu machen. Sie zielten in erster Linie auf ukrainische Dienstleister, kritische Infrastrukturen und Regierungsbehörden ab.

Diese Angriffe wurden während der ersten sechs Wochen des Konflikts fortgesetzt und dann abgeschwächt. Die meisten dieser Aktivitäten konzentrierten sich auf den Zeitraum vom 22. bis 24. Februar – also im direkten Vorfeld und während der Invasion. Diese Aktivitäten hatten durchaus Auswirkungen auf verschiedene Systeme in der Ukraine, scheinen aber letztlich keinen positiven Einfluss auf den Erfolg der russischen Landinvasion gehabt zu haben.

Ein Grund dafür kann sein, dass die ukrainische Regierung einige Tage vor diesen Angriffen viele ihrer offiziellen Online-Funktionen in eine Cloud-Infrastruktur, die von nicht an den Kämpfen beteiligten Dritten verwaltet und kontrolliert wird, verlagerte. Dadurch wurden Störungen vermieden und die Ukraine konnte viele Dienste aufrechterhalten und mit der Welt zu kommunizieren. Dies erinnert an ein ähnliches Vorgehen, als Georgien während der DDoS-Angriffe Russlands auf das Land im Jahr 2008 wichtige Regierungswebsites in Drittländer verlegt hatte.

Der Viasat-Angriff war sehr wirkungsvoll und betraf auch deutsche Windkraftanlagen
Ein weiterer zerstörerischer Angriff war die Attacke auf die Viasat-Satellitenkommunikationsmodems, die in ganz Mittel- und Osteuropa im Einsatz waren – und das gerade als die Invasion begann. Laut Raphael Satter von Reuters erklärte ein hochrangiger ukrainischer Cybersicherheitsbeamter, dass dies zu „einem wirklich enormen Kommunikationsverlust gleich zu Beginn des Krieges“ geführt habe. Dieser Angriff fügte auch NATO-Mitgliedern Kollateralschäden zu und störte unter anderem den Betrieb von mehr als 5.800 Windkraftanlagen in Deutschland.

Dies ist wahrscheinlich der wirkungsvollste aller Angriffe, die bisher während des Krieges durchgeführt wurden. In Anbetracht der Tatsache, dass die meisten Experten spekuliert haben, dass Russland einen 72-Stunden-Krieg geplant hatte, hätte eine Unterbrechung der militärischen Kommunikation bei einem Aufgehen dieser Strategie erhebliche negative Auswirkungen für die Ukraine haben können. Zudem waren die ukrainischen Kommandeure in der Lage, sich neu zu gruppieren und alternative Verbindungen herzustellen, um die Unterbrechung zu minimieren. Langfristig hat sich gezeigt, dass Russland weitaus mehr mit der Befehlskette zu kämpfen hat als die Ukraine. Vielleicht teilweise aufgrund der Unterstützung von Technologieunternehmen wie Microsoft und ESET sowie US-Geheimdiensten war der Erfolg der Ukraine bei der Abwehr zerstörerischer Angriffe beeindruckend.

Eine der raffiniertesten Malware-Bedrohungen, die auf kritische Infrastrukturen abzielten, wurde erkannt und neutralisiert, als sie im Netzwerk eines ukrainischen Energieversorgers entdeckt wurde. Die als Industroyer2 bekannte Malware war eine Kombination aus herkömmlichen Wipern, die auf Windows, Linux und Solaris abzielten, und ICS-spezifischer Malware, die auf die Betriebstechnologie (OT) abzielte, die zur Steuerung und Überwachung des Stromnetzes verwendet wird.

Microsoft hat in einem kürzlich erschienenen Bericht darauf hingewiesen, dass viele russische Cyberangriffe offenbar mit konventionellen Angriffen in Dnipro, Kiew und auf dem Flughafen Vinnytsia koordiniert wurden. Aber es gibt immer noch keine Beweise dafür, dass die Cyber-Komponente zu offensichtlichen Fortschritten in der russischen Offensive beigetragen hat.

Nach meiner Einschätzung haben destruktive Cyber-Operationen bisher so gut wie keinen Einfluss auf den Ausgang realer Kriegsgeschehnisse gehabt. Sie haben vielen Leuten zusätzliche Arbeit beschert und zahlreiche Schlagzeilen gemacht, aber was sie nicht getan haben, ist, den Krieg spürbar zu beeinflussen.

Strategie 2: Desinformation
Die Strategie der Desinformation zielte auf drei Gruppen: das Ukrainische Volk, Russland selbst und den Rest der Welt.
Russland ist kein Unbekannter darin, Desinformation als Waffe einzusetzen, um politische Ergebnisse zu erzielen. Die ursprüngliche Mission scheint einen schnellen Sieg und den Einsatz einer Marionettenregierung vorgesehen zu haben. Mit diesem Plan wäre Desinformation zunächst in zwei Einflussbereichen und im weiteren Verlauf in drei Einflussbereichen von entscheidender Bedeutung.

Das offensichtlichste Ziel ist das ukrainische Volk – es soll(te) davon überzeugt werden, dass Russland ein Befreier ist, und schließlich einen kremlfreundlichen Führer akzeptieren. Obwohl die Russen anscheinend zahlreiche Einflussnahmen über SMS und traditionelle soziale Netzwerke versucht haben, hatte dieses Vorhaben aufgrund der zunehmend patriotischen Ukraine allerdings von Anfang an kaum Erfolgsaussichten.

Russland hatte im eigenen Land, seinem zweitwichtigsten Ziel, viel mehr Erfolg mit Desinformation. Man hat ausländische und unabhängige Medien weitgehend verboten, den Zugang zu sozialen Medien blockiert und die Nutzung des Wortes „Krieg“ im Zusammenhang mit der Ukraine-Invasion kriminalisiert.

Es ist schwierig, die Auswirkungen dieser Aktionen auf die allgemeine Bevölkerung zu tatsächlich beurteilen, obwohl Umfragen darauf hindeuten, dass die Propaganda funktioniert – oder zumindest die einzige Meinung, die öffentlich geäußert werden kann, die Unterstützung der „militärischen Spezialoperation“ ist.

Das dritte Ziel der Desinformation, während sich der Krieg hinzieht, ist der Rest der Welt. Der Versuch, blockfreie Staaten wie Indien, Ägypten und Indonesien zu beeinflussen, kann dazu beitragen, sie davon abzuhalten, bei Abstimmungen der Vereinten Nationen gegen Russland zu stimmen, und sie möglicherweise dazu bringen, Russland zu unterstützen.

Propagandierte Geschichten über US-Biowaffenlabore, Entnazifizierung und angeblichen Völkermord durch die ukrainische Armee soll die Darstellung des Konflikts in den westlichen Medien in Frage stellen. Ein Großteil dieser Aktivitäten scheint eher von bereits existierenden Personen zu stammen, die Desinformationen generieren, als von kompromittierten Konten oder irgendeiner Art von Malware.

Desinformation hat eindeutig Auswirkungen, aber ähnlich wie die zerstörerischen Angriffe wirkt sie sich in keiner Weise direkt auf den Ausgang des Krieges aus. Zivilisten heißen russische Truppen nicht als Befreier willkommen, und ukrainische Streitkräfte legen weder ihre Waffen nieder noch ergeben sie sich. Die USA und Europa unterstützen die Ukraine immer noch und das russische Volk scheint vorsichtig, aber nicht rebellisch zu sein. Vor allem haben ukrainische Streitkräfte in den letzten Tagen Gebiete unter russischer Kontrolle zurückerobert und wurden sogar von einigen Zivilisten in der Nähe von Charkiw als Befreier begrüßt.

Strategie 3: Hacktivismus

Würden die bekannten, sehr erfahrenen Hacker in ganz Russland und der Ukraine zu Cyberwaffen greifen und schädliche Angriffswellen entfesseln, die jeweils die eigene Seite unterstützen? Es sah ganz danach aus, als ob das zu Beginn des Kriegs der Fall sein könnte.

Einige bekannte Cybercrime-Gruppen wie Conti und Lockbit erklärten sofort, sie seien für die eine oder andere Seite, aber die meisten von ihnen erklärten, dass es ihnen egal sei und sie wie gewohnt weitermachen würden. Aber wir haben einen deutlichen Rückgang der Ransomware-Angriffe etwa sechs Wochen lang nach der ersten Invasion beobachtet. Das normale Volumen der Angriffe wurde Anfang Mai wieder aufgenommen, was darauf hindeutet, dass die Kriminellen genau wie der Rest von uns Unterbrechungen in der Lieferkette hatten.

Eine der berüchtigtsten Gruppen, Conti, gab auf ihrer Leak-Site Droherklärungen gegen den Westen ab, was dazu führte, dass ein ukrainischer Forscher ihre Identität und Praktiken preisgab, was schließlich zu ihrer Auflösung führte.

Andererseits liefen Hacktivisten auf beiden Seiten in den frühen Kriegstagen zu Hochtouren auf. Web-Defacements, DDoS-Angriffe und andere triviale Hacks zielten auf so ziemlich alles

ab, was angreifbar und eindeutig als russisch oder ukrainisch identifizierbar war. Die Phase dauerte aber nicht lange und scheint keine nachhaltige Wirkung zu haben. Nachforschungen zeigen, dass diese Gruppierungen sich schnell langweilten und zur nächsten Ablenkung übergingen. Auch hier führten die Aktivitäten also nicht zu materiellen Auswirkungen auf den Krieg – wohl aber zu Pranks, für die sich die jeweiligen Hacktivisten gefeiert haben dürften. Vor kurzem hat zum Beispiel ein Gruppe angeblich Yandex Taxi gehackt und alle Taxis ins Zentrum von Moskau bestellt, was zu einem Stau führte.

Kategorie 4: E-Spionage
Die letzte Kategorie ist am schwierigsten zu quantifizieren, da es per se kompliziert ist, die Auswirkungen von etwas zu beurteilen, das von Natur aus verdeckt ist. Die erfolgversprechendste Methode abzuschätzen, wie umfangreich Spionage in diesem Krieg ausgeführt wurde, besteht darin, sich die Zeiten anzusehen, in denen die Versuche entdeckt wurden. Im Anschluss kann der Versuch starten, zu extrapolieren, wie oft Versuche erfolgreich gewesen sein könnten, wenn man bedenkt, wie oft sie es nicht waren.

Im Gegensatz zu zerstörerischen Angriffen sind E-Spionageangriffe aufgrund ihres verdeckten Charakters und der damit verbundenen Schwierigkeit, sie zuzuordnen, nützlich gegen alle gegnerischen Ziele, nicht nur gegen die Ukraine. Wie bei der Desinformation gibt es in diesem Bereich weitaus mehr Aktivitäten, die auf die Unterstützer der Ukraine abzielen, als andere Arten von Angriffen, die die Verbündeten der USA und der NATO in den Bodenkrieg einbringen könnten.

Behauptungen über Angriffe auf nicht-ukrainische Unternehmen müssen sorgfältig geprüft werden. Es ist nichts Neues, dass Russland die Vereinigten Staaten, die Europäische Union und weitere NATO-Mitgliedstaaten mit Malware, Phishing-Angriffen und Datendiebstahl attackiert, allerdings gibt es in einigen Fällen überzeugende Beweise dafür, dass Angriffe speziell durch den Krieg in der Ukraine motiviert sind.

Im März 2022 veröffentlichte die Threat Analysis Group (TAG) von Google einen Bericht, in dem auf russische und weißrussische Phishing-Angriffe hingewiesen wurde, die auf in den USA ansässige Nichtregierungsorganisationen und Think Tanks, das Militär eines Balkanlandes und einen ukrainischen Rüstungskonzern abzielten. Proofpoint veröffentlichte ebenfalls Untersuchungen, die zeigen, dass EU-Beamte, die an der Unterstützung von Flüchtlingen arbeiten, Ziel von Phishing-Kampagnen waren, die von einem ukrainischen E-Mail-Konto ausgingen, das angeblich zuvor vom russischen Geheimdienst kompromittiert worden war.

Russische Angriffe auf ukrainische Ziele haben in den letzten sechs Monaten nicht nachgelassen und nutzen immer wieder die neuesten Sicherheitslücken aus, sobald sie öffentlich bekannt gegeben wurden. Im Juli 2022 gehörte beispielsweise eine in Russland ansässige Cybercrime-Gruppe zu den Hauptakteuren, die eine neue Schwachstelle in Microsoft Office mit dem Namen „Follina“ umfassend nutzten. Es scheint, dass eines der Ziele für bösartige Dokumente in dieser Kampagne Medienorganisationen waren – ein wichtiges Werkzeug während eines Krieges.

Fazit
Der Krieg in der Ukraine lehrt uns viel über die Rolle, die Cybersicherheit und Cyberangriffe in Kriegszeiten spielen können. Russland war scheinbar nicht ausreichend vorbereitet und hätte Cyberangriffe weit wirkungsvoller einsetzen können.

Die frühen Stadien des Krieges schienen sich auf Destabilisierung, Zerstörung und Störung zu konzentrieren und basierten auf der Annahme eines schnellen Sieges durch Russland. Da sich der Krieg allerdings immer weiter hinzieht, verlieren diese Techniken an Bedeutung, und der Schwerpunkt liegt vermehrt auf Spionage und Desinformation.

Es bleibt abzuwarten, wie sich die Dinge in den kommenden Monaten vor dem Hintergrund der Energieversorgung und Russlands dominanter Rolle in diesem Bereich entwickeln werden. Wird die Desinformation einen höheren Gang einlegen, um Druck auf die europäischen Staats- und Regierungschefs auszuüben, die Sanktionen aufzuweichen? Werden sich kriminelle Gruppen auf Angriffe auf europäische Energieversorger konzentrieren, wie wir es bereits in kleinem Maßstab erlebt haben?

Der Krieg ist noch nicht vorbei und die Rolle von Cyberangriffen kann sich auf neue und unvorhergesehene Weise entwickeln. Unwahrscheinlich ist, dass sie eine entscheidende Rolle spielen wird. Zumindest in diesem Konflikt ist es ein weiteres Werkzeug, das in Verbindung mit anderen Waffen und Kriegswerkzeugen verwendet werden muss – und wie bei jedem anderen Aspekt des Krieges ist eine starke Verteidigung oft die beste Offensive.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de