Bear in the Net: A Network-Focused Perspective on Berserk Bear

blog.gigamon.com/2021/10/25/bear-in-the-net-a-network-focused-perspective-on-berserk-bear/

October 25, 2021

Threat Research / October 25, 2021

Joe Slowik &nbsp

Berserk Bear is one of many names for a threat actor operating since at least 2010. Alternatively referred to or encompassing operations tracked as Crouching Yeti, Dragonfly, and Iron Liberty, among others, the group is linked by multiple entities to Russian state-directed operations. Throughout over a decade of activity, Berserk operated in a variety of sensitive environments, from industrial organizations to government entities – but without any apparent, direct impact.

While recently published research indicates this group may be responsible for inadvertent disruption as part of its activities in critical infrastructure environments, even absent such impacts Berserk's behaviors are cause for concern. Viewed potentially as preliminary operations necessary for future cyber impacts, Berserk represents a preparatory agent enabling future, more worrying events.

The implications of Berserk activity for critical infrastructure owners and operators are significant. Although not directly linked to any known, intended disruptive or destructive event, the group's operations cover all necessary steps to position an adversary for such an operation in the future. For network defenders, a review of this group's actions is therefore not merely helpful but for some necessary to guard against this type of threat. In this post, we will examine network-focused items related to Berserk Bear operations throughout the group's history as detailed in recently published research.

Exploit to Credential Leak

Initial Berserk activity, often referred to as the Dragonfly Campaign, utilized exploits as part of multiple intrusion vectors to gain initial access to victims from at least 2010 through 2014. After a brief period of quiet, the group returned to action using superficially similar initial access mechanisms: strategic website compromise (SWC) and phishing campaigns with malicious attachments. However, unlike earlier activity, post-Dragonfly operations avoided the use of exploits and instead focused on leaking credentials from victim machines.

Through either reference to external objects in malicious documents or by injecting a reference to a remotely hosted object in an otherwise legitimate webpage, Berserk operators worked to harvest credentials by prompting an external authentication attempt from victim machines. Similar to penetration testing techniques such as use of the Responder tool for capturing logon information, the technique prompts a victim machine to initiate an outbound Server Message Block (SMB) query to retrieve a remotely-hosted file object. As part of this communication, Windows authentication information (the username and NTLM hash) passes to the remote machine, which an intruder can capture for future replay.

From a defender's perspective, the first recommendation to avoid such information leakage is to deny outbound SMB connections (TCP 445). Where such actions are not possible, external connectivity should be limited to known-necessary networks. Alternatively, such traffic can be rigorously logged as SMB communications can be leveraged for a variety of malicious actions beyond the credential leak activity associated with Berserk Bear.

When SMB routes fail, Windows will fail-over to Web Distributed Authoring and Versioning (WebDAV) to retrieve the same resource via HTTP. The fail-over communication can be identified in network traffic via a WebDAV-containing user agent string. Monitoring HTTP traffic containing a WebDAV-related user agent can reveal these attempts when outbound SMB traffic is blocked or filtered. While this alone may be insufficient to identify truly suspicious traffic as legitimate use cases exist, pairing with analysis of infrastructure or originating application or resource can reveal instances worth further investigation.

Abusing Remote Access

Post-Dragonfly actions associated with Berserk used harvested credentials for both remote access to victim environments and lateral movement inside compromised networks. More recent campaigns linked to this entity continue to emphasize credential harvesting, leveraging a combination of exploits, tools, and standard collection techniques as means to access logon information. Overall, just as Berserk transitioned from exploits for initial access, consistent credential gathering and reuse allows the intruder to blend in with normal user activity and evade easy detection.

Once inside victim networks, Berserk actors create adversary-controlled administrator accounts and modify system settings to facilitate follow-on access, as well as continuous password theft and cracking to gather more existing account information. While other techniques also appear in Berserk-related campaigns in the late 2010s, Berserk operations from 2018 to the present focus on having steady, reliable access to valid credentials. Berserk then leverages collected credentials for remote access, lateral movement, as well as for tactics such as remote process execution using the PSExec tool.

A variety of host-centric controls exist to monitor or limit these techniques. First and foremost, network owners must deploy and enforce robust multi-factor authentication (MFA) schema to significantly minimize the risk of account compromise and credential reuse.

Additionally, defenders can monitor system and access logs for unusual activity associated with specific user accounts, and audit privileged account use within the network.

In addition to these host-based operations, network-centric options also exist to monitor and track possible credential abuse. For example, especially where host-centric logs may not be easily accessible or available, mapping authentication pairs – source and destination system – and associated accounts can identify overall patterns in network traffic. While potentially overwhelming and unwieldy for covering all remote authentication activity, focusing on external-to-internal behaviors to track new authentication sources or emphasizing “high value” internal targets (domain controllers, security tools, or industrial systems) can yield potentially valuable results. Identifying a new, not previously seen remote access attempt to the network from an unfamiliar network address (discussed further below) can be the first touchpoint revealing potential credential loss and a follow-on intrusion attempt. Similarly, identifying authentication attempts to critical assets from standard user machines in the network can reveal opportunistic lateral movement activity.

Expanding beyond authentication tracking, defenders can utilize network visibility to enhance understanding of file movement and process execution as well. Similarly reliant upon credential access, looking for activity such as share mapping (and subsequent file movement) or remote process execution via various frameworks is critical to mapping lateral movement activity. Identifying unusual relationships in such activity, such as file movement directly between workstations or remote process activity outside of policy and administration parameters can reveal adversary operations in progress.

Certainly, none of the above items are easy to implement, but represent necessary steps for network owners and defenders to evolve with adversaries such as Berserk Bear. Luckily, advances in technology, modeling, and threat analysis mean defenders can take advantage of robust, mutli-faceted detection of systemic anomalies to reveal adversaries attempting to “blend in” with normal system operations.

Infrastructure Capture for Communications

Berserk Bear is interesting not just for its activity, but also the nature of the *infrastructure* used to carry out that activity. Starting with the Dragonfly campaign, Berserk utilized compromised, legitimate sites and services for operations. By the later Palmetto Fusion campaign and follow-on activities, Berserk shifted almost entirely to using compromised infrastructure for malicious activity.

When procuring network infrastructure, adversaries have two general choices: they can create their own (lease IP addresses and servers, register domain names, etc.) or leverage a third party’s existing service. One of the more direct ways of achieving the latter is to simply compromise someone’s vulnerable system for use in attacks, whether for botnets or as proxy nodes for communication. For an adversary, this approach can evade typical defender analysis and pivoting methodologies by avoiding creation patterns or relative “newness” of registered domains.

Yet opportunities still exist to differentiate communication pathways provided defenders can enrich and contextualize these observations. Looking at previously described Berserk behaviors, such as credential harvesting and follow-on remote access, even if this activity involves a compromised, otherwise legitimate server, defenders can still identify suspicious characteristics in the infrastructure to power security-driven decision-making. For example, defenders can establish profiles of remote access to the monitored network including not just geography but also service providers and even Autonomous System Numbers (ASNs) for clients. Using this information to then identify items outside the norm, such as the expanded anomaly approach described previously, or establishing allow-lists preemptively to block activity outside of existing patterns can defeat activity such as Berserk.

Expanding on this, for remote access activity such as connection to the corporate VPN or remote access technologies such as RDP or SSH, activity coming from a remote user would likely originate from an Internet Service Provider (ISP) catering to home users. Observing such remote access activity from a virtual public server (VPS) or cloud service provider would be very strange – but also represents a likely pathway for an entity compromising third-party infrastructure for use as communication relays. By enriching and understanding communication nodes – essentially, viewing network observables as composite objects – defenders can build context around observed IP addresses and other items to make security-focused decisions.

Conclusion

Berserk Bear, in many respects, represents a historical entity in that no publicly known operations have been attributed to this group since 2020. While some may assume this group would therefore offer little to defenders right now in terms of lessons learned, closer investigation reveals Berserk deploying a variety of tactics and techniques that mirror behaviors associated with current ransomware and other advanced persistent threat entities.

By researching and analyzing Berserk Bear campaigns, defenders can gain significant insight into adversary tradecraft aligning with abuse of legitimate services and “living off the land” techniques. Furthermore, understanding is necessary for defenders to take the next required step: building and deploying detections and defenses against such behaviors.

Network defenders and system owners can use this iterative process of threat analysis and defense development far more widely. By first understanding how given adversaries operate, then identifying various detection and identification opportunities associated with observed capabilities and actions, defenders can ensure coverage of adversary tradecraft. Analysts can then expand from specific instantiations of tradecraft to more general understanding of the fundamental behavior for broad-scope defense meeting wider developments across multiple adversaries.

Tell us your favorite security resource for a chance to win a $100 Amazon Gift Card

Winners will be drawn on November 1st. To learn more about this contest, visit the Community.

Gigamon® | Community

CONTINUE THE DISCUSSION

People are talking about this in the Gigamon Community's Security group.

Share your thoughts today

NDR Resource

RELATED CONTENT

REPORT

2022 Ransomware Defense Report

GET YOUR COPY >

WEBINAR

ThreatINSIGHT: Eliminating Adversaries' Dwell Time Advantage

WATCH ON DEMAND >

WEBINAR

Deep Dive INSIGHTS: Fighting Ransomware and Shifting Security Priorities

WATCH ON DEMAND >

OLDER ARTICLE

Gigamon Community Member Spotlight: Indera Budiman Bin Wahabi

NEWER ARTICLE

Overcome Cloud Pain Points with Hybrid Traffic Intelligence

↑ TOP