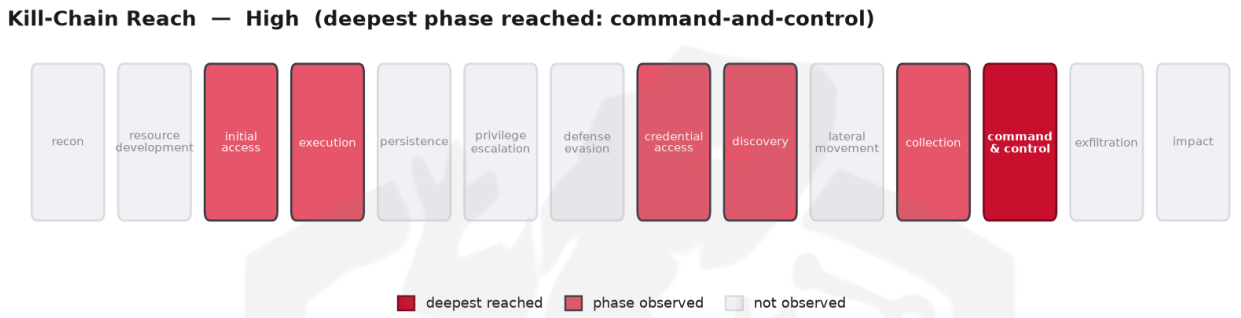
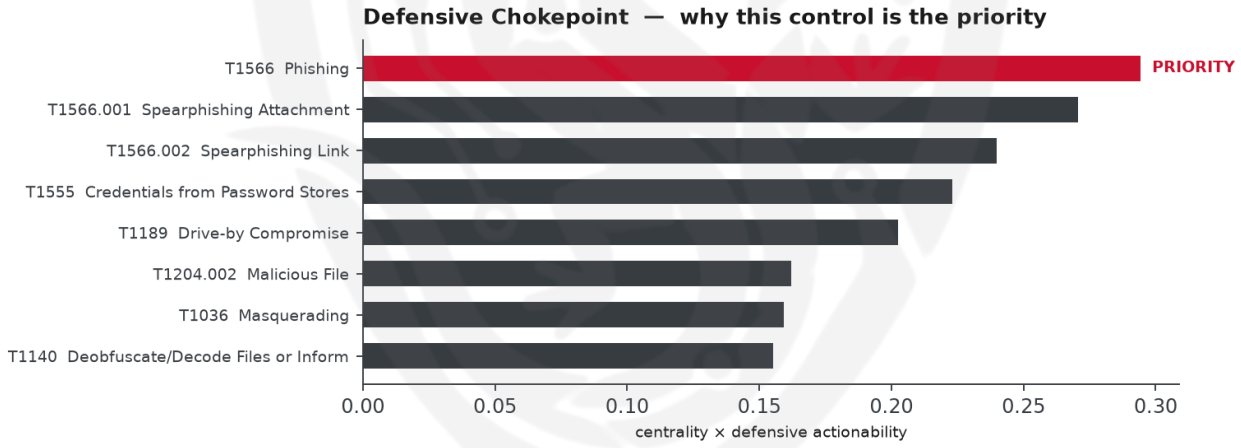
THREAT REPORT: BORYPTGRAB STEALER DEPLOYMENT VIA GITHUB IMPERSONATION

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The observed cluster of activity involves the deployment of the BoryptGrab Stealer malware, targeting unspecified sectors and countries. The threat actor utilizes various techniques, including phishing and keylogging, to compromise systems. Priority should be given to enabling defensive measures against phishing attacks, as this is identified as the primary technique used by the threat actor. The lack of specific attribution and targeted sectors makes it essential to focus on the technical aspects of the attack to develop effective countermeasures.

Threat Overview

The threat actor, whose identity is currently insufficient to determine, is deploying the BoryptGrab Stealer malware. This malware is used to steal information from compromised systems, leveraging techniques

such as keylogging, stealing web session cookies, and masquerading as legitimate resources. The victimology of this campaign is not well-defined due to insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The attack chain involves a series of techniques aimed at compromising systems and stealing sensitive information. This includes phishing (T1566), which is identified as the priority technique, indicating that phishing is a critical point in the attack chain. The priority control, as recommended, is to "Enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button." This measure directly addresses the primary technique used by the threat actor, aiming to mitigate the risk of initial compromise.

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in relation to this campaign. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence level of 80% or higher. This lack of corroboration highlights the need to rely on the technical analysis of the attack chain and the recommended priority controls to defend against this threat.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1036 Masquerading
- T1083 File and Directory Discovery
- T1566 Phishing
- T1027 Obfuscated Files or Information
- T1518.001 Security Software Discovery
- T1189 Drive-by Compromise
- T1518 Software Discovery
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2943).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6136; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
Darkhotel	0.6136
Ajax Security Team	0.5657
Windshift	0.5477
PLATINUM	0.5196
Elderwood	0.5164

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator
URL	hxxps://bentleyvazquezpvey[.]github[.]io/[.]github/
URL	hxxps://github[.]com/Arctic-Wolf-Security
URL	hxxps://github[.]com/antivirus-free-bitdefender
URL	hxxps://github[.]com/malwarebytes-protection
Hash	b98575f3c0259b480a31b917aa73bc56
Hash	fd01262bd56510088b9ddfe58ca101ab

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1566 Phishing (initial-access)
- **Observed here:** T1566 Phishing was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 38+ groups that use Phishing, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1203 Exploitation for Client Execution to maintain their objective by leveraging vulnerabilities in client applications, such as browsers or Office software, which may be exposed if the initial phishing attempt was intended to establish a foothold. This technique may be particularly appealing as it allows the actor to execute malicious code on the client-side, potentially bypassing some security controls, and could be used to deliver a payload or establish a backdoor. The defensive countermeasure to mitigate this potential pivot would be to patch client applications, enable exploit mitigations such as ASLR, DEP, and CFG, and implement application isolation.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=43, lift 1.3), T1106 Native API (n=18, lift 1.6)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
  - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
  - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
  - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log