Larry L. Sautter 2019 Award Application

1. Project title: **UC Davis Email Security and Infrastructure Modernization**

2. Submitter's name, title, and contact information:

Thomas Pomroy

Information Architect, UC Davis IET

tepomroy@ucdavis.edu

3. Names of project leader(s) and team members:

Project Sponsor:

Michael Khan, Associate CIO, Information and Educational Technology

Project Team / Key Contributors:

Thomas Pomroy, Information Architect
Vincent Fox, Enterprise Infrastructure
Peter Carroll, Enterprise Email
Joshua Van Horn, Enterprise Services Manager
Matt Wilson, Application Architect
Jon Mortimer, Systems Administrator
Jeff Rowe, Information Security
Rick Leos, Systems Administrator
Joseph Crain, Application Architect
Chris Callahan, Enterprise Infrastructure
Justin Earley, Systems Administrator
Ernie Comer, Project Manager

4. Project Summary: Over the past three years, UC Davis has leveraged cloud-based solutions and internet standards to enhance security and reliability of email services offered to faculty, students and staff. Deprecation of frequently attacked legacy services, and broad implementation of multi-factor authentication, led to dramatic drops in compromised accounts and abuse of university resources.

5. Project Narrative:

Background

UC Davis is nearing the end of a long journey of email consolidation.

In 2000, the campus had dozens of email services at the department level, owing to a need for collaborative calendaring and larger email quotas not offered by the traditional central email service. By 2008 the central service

was collapsing under its own costs, while at the same time not meeting the needs of customers. In 2009, Google's cloud-based email was implemented for undergraduates, relieving cost pressures but not providing a consolidated collaboration platform for business and administrative needs. On-prem Exchange services were many, and the central offering was prohibitively expensive for many units. In 2014, Office 365 was implemented and centrally financed, causing a flood of consolidation of department-run services: the last two department-run Exchange services moved to Office 365 in 2018. More than 95% of faculty, students and staff now receive campus email in the centralized Office 365 or DavisMail services, with fewer than 1% taking delivery to department-run mail services.

Why this matters:

Consolidating these services saves considerable staff resources in the aggregate, and provides a consistent, professionally run service for customers. Staff can easily collaborate by scheduling meetings, sharing documents via cloud storage, etc. Issues of legal retention and discovery are handled easily. Authentication is consolidated in campus-wide standards. Misconfigurations of servers run by part-time administrators have largely disappeared. Consolidation eases adoption of reputation enhancements like DKIM signing of outbound messages; this enhances deliverability, which is crucial to development/advancement and other outreach efforts. Multi-factor authentication can be configured and maintained in one place by a few employees, providing crucial security for 21st century services that are increasingly available anywhere and aren’t protected by our own firewalls.

Project Description

Increase security of email service and campus credentials against phishing and exploitation; facilitate collaborative work tools and information-sharing on common platforms; make long term plans for affordable, supportable, sustainable email services; burnish the reputation of internet-directed email sent by UC Davis.

What we accomplished

Retired Cyrus (October 2016)

- Ended offering of outdated, expensive, on-prem email hosting.

Retired legacy MX routing and hygiene pool (2019)

- Routed all email domains to Exchange Online.
- Ended bespoke email hygiene processes in favor of supported industry standard tools.

Deprecated and secured legacy SMTP pool (2018-2019)

- Finding that less than 1% of the 196,000 IP addresses on campus needed access to the service to send unauthenticated messages, we disabled access to all but 1900 of them.
- Finding that less than 4% of the 18,000 users with access to send authenticated email via the SMTP pool were actually using it, we disabled the service for those users, leaving it active for only 675.Worked with campus IT staff to identify alternatives to the legacy SMTP pool including using Microsoft Exchange Online as the SMTP service. Identified users and hosts still using the service and communicated them to IT staff.
- Worked with campus IT staff to identify alternatives to the legacy SMTP pool including using Microsoft Exchange Online as the SMTP service. Identified users and hosts still using the service and communicated them to IT staff.

Migrated thousands of users to centrally run services (Office 365, DavisMail) (2016-2019)

- Consolidated 90%+ staff and faculty on single service (Office 365)
- Consolidated all undergraduate students on single service (DavisMail)

Implemented Duo MFA for email services (2017-2019)

- Made Duo MFA for email available October 2017
- Mandate from the chancellor pushed Duo enrollment for Office 365 to 53% of faculty and staff.

Implemented ATP advanced protection for email services (2018)

- Additional anti-phishing layer for attachments and links

Implemented email reputation policies (2018)

- DMARC authentication and reporting
- SPF authentication for third-party services, campus services
- DKIM signatures for major email services

How do we know this work has been effective?

Large public universities, due to their open, collaborative architectures and often de-centralized, research focused activities, are consistently a target of attack by malicious actors. While no email service can be said to be completely secure, the steps we've taken so far have proved to be a strong deterrent to even determined attack groups.

Information Security Office Case Study

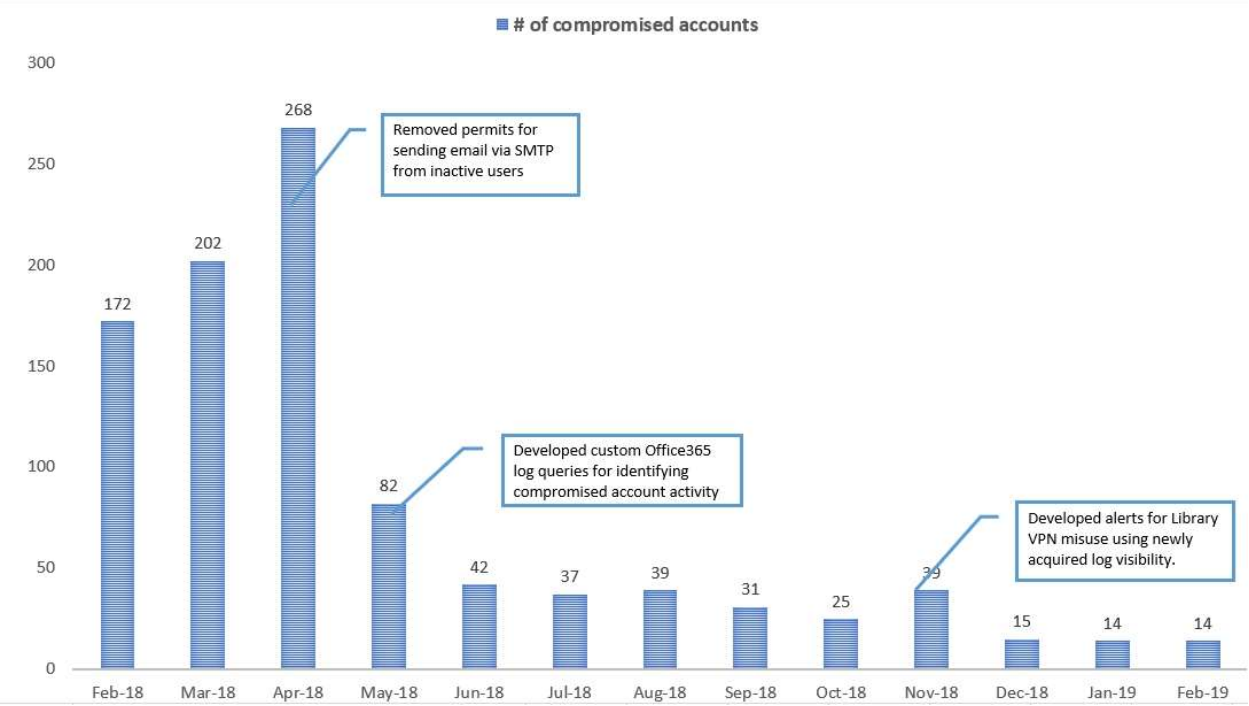
Starting in December 2017, UC Davis became increasingly targeted by the Black Axe hacker group [1]. We learned this by correlating activity in compromised account logins with other sources of threat intelligence. Further investigations indicated that the same phishing infrastructure used to attack UC Davis was being used to target many universities.

The hacker group's primary method was to send internal UC Davis email from previously compromised UC Davis computing accounts. Campus recipients received phishing emails sent by apparently legitimate campus users from legitimate campus systems. This tactic allowed the attackers to recursively gather increasing numbers of compromised accounts. Removing the capability of most campus users to send arbitrary SMTP email messages through the on-premise email system severely reduced the attackers' ability to gather account credentials via internal email campaigns. However, the Office 365 online email system still permitted targeted, low-volume phishing and spear-phishing campaigns. The Black Axe group quickly pivoted to this alternate strategy. We identified high-

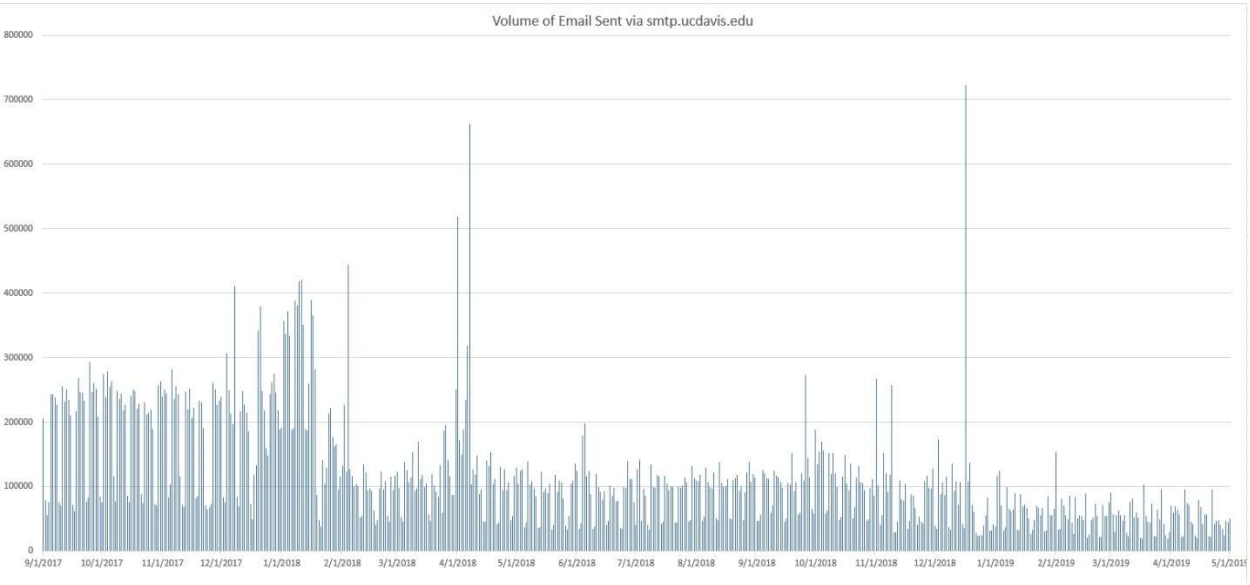
fidelity email transaction rules observable in the Office 365 OMS log search portal that identified attacker behavior prior to sending phishing campaigns. We used this insight to aggressively lock the compromised accounts. The hacker group quickly pivoted again and used the compromised UC Davis accounts to launch phishing attacks against other universities. In this final strategy, the attackers used the UC Davis Library VPN, available to all users to access academic journals off-campus, to send emails to victims at other universities. This was successful because other institutions could not block email from UC Davis without denying legitimate communications between campuses. We used our newly developed Elasticsearch security logging system to gain visibility into UC Davis Library VPN activity. Since VPN access is based upon the installation of PC client software, we gleaned a wealth of useful intelligence into the attacker activity, including their computer names and the platforms used in the attacks. This information was turned into high-fidelity signatures that further identified compromised campus computing accounts, which were subsequently locked. Currently we see very little activity attributable to the Black Axe hacker group. The remaining rate of account compromise exhibits no clear coordination or organized efforts.

[1] https://www.wired.com/story/nigerian-email-scammers-more-effective-than-ever/

1 The effects of infrastructure changes on compromised accounts



2 Overall SMTP pool sending volume over time.



Conclusion / What's next?

Through best practices, retirement of older services, and leveraging of cloud-based tools, we can now provide better, more secure email services to UC Davis customers. Email remains the primary method of communication in our

environment, and the steps we've taken will keep it relevant and useful as a tool for business and education going forward.

Our approach of harm reduction through reducing surface attack spaces and enrolling users in multi-factor authentication has already started causing attackers to look elsewhere for easier targets. As we continue these efforts and add additional layers of security we should continue to see the positive impacts of this work.

Opportunities remain for proactive work with email security. We are on a path towards adding DMARC compliance to determine the authenticity of email purported to be from UC Davis senders, including third-party vendors with whom UC Davis does business. We've begun to work actively with staff to ensure inbox deliverability for crucial business and fundraising messages. We're constantly examining our security models for ways to improve the quality and integrity of the service, and to simplify administration for IT staff.